Internal Control Provisions of the Department of Homeland Security Financial Accountability Act

Implementation Guide

Exposure Draft
Fiscal Year 2005

Homeland
Security

This guide is designed to assist the Department in its efforts to satisfy its responsibilities established by the internal control provisions of the Department of Homeland Security Financial Accountability Act (P.L. 108-330). The guide is based on rule-making and guidance available as of April 28, 2005. Accordingly, as new rules or modifications or interpretations to existing rules emerge, certain aspects of this guide may become obsolete. Because interpreting this guidance is proving to be an evolutionary process, preparers and users are cautioned to carefully evaluate and monitor further implementation guidance from the Department's Office of Financial Management.

“Effective Internal Control is the Key to Accountability”

Andrew Maner
Chief Financial Officer

U.S. Department of Homeland Security

Table of Contents

Appendices

Executive Summary

Introduction

On October 16, 2004, the President signed into law the Department of Homeland Security (DHS) Financial Accountability Act (hereinafter referred to as the DHS Financial Accountability Act). The DHS Financial Accountability Act requires the Secretary of Homeland Security to include in the Performance and Accountability Report (PAR) for fiscal year 2005, an assertion on internal control over financial reporting. Starting in FY 2006 and for fiscal years thereafter, the Secretary must include in the PAR, an audit opinion on the Department of Homeland Security's (the Department) internal controls over financial reporting.

In addition, the revised OMB Circular No. A-123, *"Management's Responsibility for Internal Control"*, provides specific requirements for federal agencies to establish internal controls, assess internal controls, correct internal control deficiencies and report on internal controls. The circular requires federal agency managers to incorporate basic internal controls in the strategies, plans, guidance and procedures that govern their programs and operations.

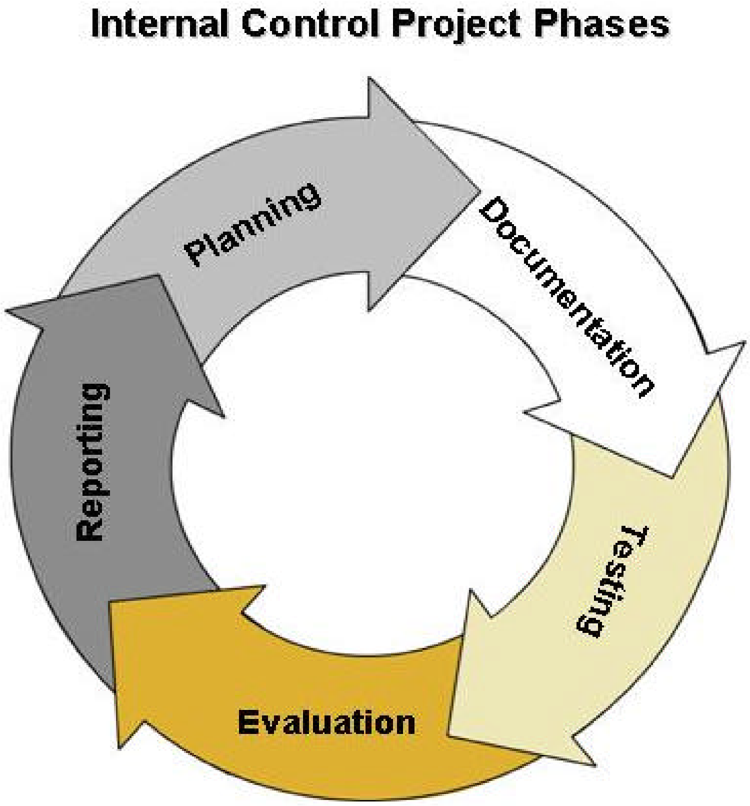
Compliance with the internal control requirements over financial reporting will be interpreted and refined as it progresses through the federal government community. This guide is the initial interpretation on how best DHS can support the requirements related to the DHS Financial Accountability Act.

This executive summary provides an overview of the methodology for implementing the internal control provisions of the DHS Financial Accountability Act and outlines key issues to be considered in using the methodology.

Project Initiation

Project Initiation identifies the parties charged with project oversight, the line of business integration and management, and project management. Project management establishes accountability, identifies deadlines, and sets consistent standards for execution & remediation, and communication channels.

Figure 1: Internal Control Project Phases



Planning Phase

The Planning Phase section describes the methods to plan for an internal control project. The Planning Phase will involve a top-down approach to determine the documentation necessary and the nature, timing, and extent of testing of controls to be performed for each significant line item and related account, disclosure, and process at each of the organizations' Components.

Documentation Phase

The Documentation Phase section describes the format of documents produced to form the basis and support for management's assessment of internal control over financial reporting. The Component Assessment Teams will determine the scope of documentation, prepare walkthroughs for each process, develop control documentation, and document their assessment of the design and operational effectiveness of controls.

Testing Phase

The Testing Phase section discusses what is required to test controls that are effectively designed. Controls are tested to ensure the controls are functioning properly. Testing is also necessary to support management assertion of the controls. This requires testing the controls, which must include each of the five Components of internal control over all relevant assertions for all significant line items and related accounts, and disclosures at each individually important DHS Component and over the specific risk areas at other DHS Components. The detailed test plan includes identification of controls to be tested, coordination and assignment of testing procedures, and a plan for test execution. The execution plan should identify how to test the controls, how to document and evaluate the results, and identify deficiencies. Once a plan is in place, testing is executed.

Evaluation Phase

The Evaluation Phase section describes the manner in which the Component Assessment Teams will identify, assess, and classify internal control deficiencies identified as a result of the testing of those controls. Identification and assessment involve determining whether a deficiency is remote or inconsequential by assessing the magnitude and likelihood of misstatement. Based on the assessment, deficiencies are classified as material weakness, reportable condition, or control deficiency.

Reporting Phase

The Reporting Phase section describes procedures for reporting, including reporting requirements of the Components, Internal Control Committee (ICC) Board, Senior Management Council, Secretary, and other matters related to reporting. The Reporting Phase is the last phase of the internal control assessment process. The DHS Financial Accountability Act and OMB Circular A-123 require DHS to report an annual assurance statement for internal control over financial reporting, material weaknesses, and the auditor’s opinion externally in the PAR.

Conclusion: Priorities for the Future

DHS will continue to strive for the highest quality financial management in our commitment to effective internal controls in support of reliable and timely financial data to support management decisions. The DHS ICC will continue to define the strategy and vision to achieve full compliance with internal control over financial reporting provisions of the DHS Financial Accountability Act. Creating a strategy, in many respects, is about setting priorities and recognizing that some actions are more critical or more urgent than others in achieving our goals. The ICC will continue to identify high priority areas for additional resources and attention in support of the strategy for internal controls in future years.

SECTION ONE: Introduction

Purpose and Scope

This introduction provides an overview of the internal control provisions of the Department of Homeland Security Financial Accountability Act and OMB Circular A-123, as revised. It also provides fundamental concepts and government standards for internal controls over financial reporting, along with background information regarding additional laws affecting internal control and its history within the federal government.

1.1 – Summary of the Internal Control Provisions of the Department of Homeland Security Financial Accountability Act

The Department of Homeland Security Financial Accountability Act (P.L. 108-330), hereinafter referred to as the DHS Financial Accountability Act) requires the Secretary of Homeland Security, among other things, to:

- Include in the FY 2005 Performance and Accountability Report (PAR):
  - An assertion of the internal controls that apply to financial reporting.

- Include in the FY 2006 PAR and thereafter:
  - An audit opinion of the Department's internal controls that apply to financial reporting.

- Design and implement Department-wide internal controls[1] that reflect the most recent Homeland Security Strategy and permit assessment, by the Congress and by managers within the Department, of the Department's performance in executing such strategy.

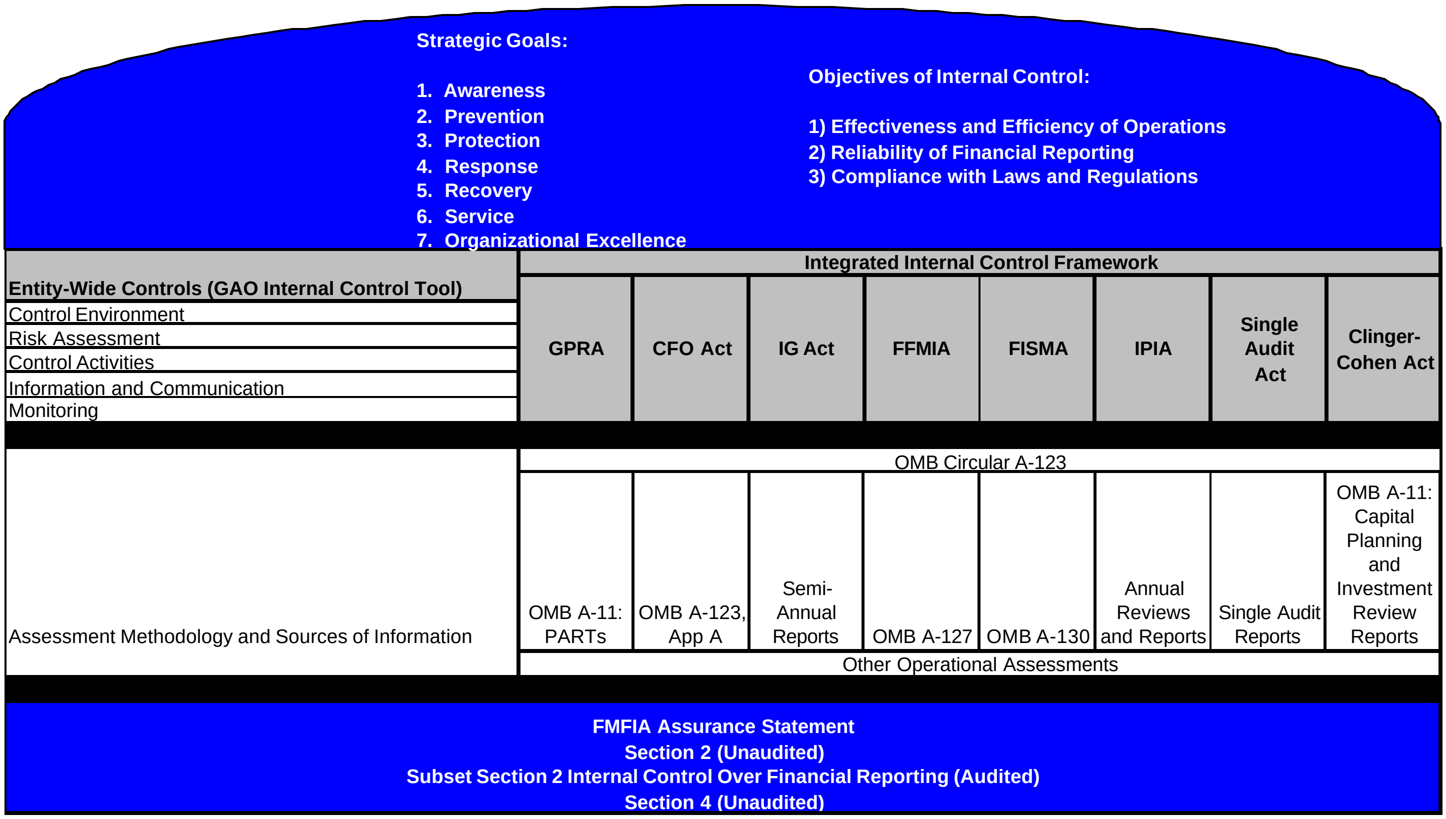
Refer to Appendix B of this guide for a full copy of the DHS Financial Accountability Act. Section 4 of the DHS Financial Accountability Act provides that compliance of the Act is a function of the Chief Financial Officer. Ultimately, the Secretary's statement of assurance for internal control over financial reporting will be reported as a subset of the overall statement of assurance as required by Section 2 of the Federal Managers' Financial Integrity Act.

The implementation guide does not provide a process for the provision of the DHS Financial Accountability Act related to the design and implementation of Department-wide management controls. The Department is currently developing an integrated internal control framework for all objectives of internal control and plans to work closely with OMB to provide further implementation guidance. These plans will be implemented in FY2006. The graphic below depicts the Department's integrated internal control framework currently under development.

[1] Per the revisions made to OMB A-123, throughout the circular "management controls" was changed to "internal control" to "better align with currently accepted standards for internal control and current terminology. The terms are intended to be synonymous."

Figure 2: FMFIA and Internal Control Provisions of the DHS Financial Accountability Act Framework

**Federal Managers' Financial Integrity Act (FMFIA) and
Internal Control Provisions of DHS Financial Accountability Act
Framework**



Strategic Goals:

1. **Awareness**
2. **Prevention**
3. **Protection**
4. **Response**
5. **Recovery**
6. **Service**
7. **Organizational Excellence**

Objectives of Internal Control:

1) Effectiveness and Efficiency of Operations
2) Reliability of Financial Reporting
3) Compliance with Laws and Regulations

Entity-Wide Controls (GAO Internal Control Tool)	**Integrated Internal Control Framework**							
Control Environment Risk Assessment Control Activities Information and Communication Monitoring	**GPRA**	**CFO Act**	**IG Act**	**FFMIA**	**FISMA**	**IPIA**	**Single Audit Act**	**Clinger-Cohen Act**
Assessment Methodology and Sources of Information	OMB Circular A-123							
	OMB A-11: PARTs	OMB A-123, App A	Semi-Annual Reports	OMB A-127	OMB A-130	Annual Reviews and Reports	Single Audit Reports	OMB A-11: Capital Planning and Investment Review Reports
	Other Operational Assessments							

FMFIA Assurance Statement
Section 2 (Unaudited)
Subset Section 2 Internal Control Over Financial Reporting (Audited)
Section 4 (Unaudited)

1.2 – Goal of DHS Internal Control Assessment Guide

The goal of this implementation guide is to enable the Department to:

- Provide an assertion over the effectiveness of the internal controls over financial reporting as mandated by the DHS Financial Accountability Act;

- Assess internal control in a manner which would allow the Department to meet the audit requirements to support an attestation on internal control over financial reporting[2]; and

[2] The current Audit Standard for Reporting on Internal Controls over Financial Reporting is Statement on Standards for Attestation Engagements (SSAE) No. 10, Chapter 5 Reporting on an Entity's Internal Control over Financial Reporting, commonly referred to as AT501. The standards are promulgated by the American Institute for Certified Public Accountants (AICPA) Auditing Standards Board (ASB). The ASB is currently in the process of revising the standard and has published an exposure draft for comment. The final revision is expected to include similar requirements of the auditors and management for internal control over financial reporting as those of Auditing Standards No. 2 (AS2) published by the Public Company Accounting Oversight Board (PCAOB) in order to meet the requirements of The Sarbanes-Oxley Act of 2002.

- Comply with the revisions to OMB Circular A-123, Appendix A.

1.3 – History of Internal Control in the Federal Government

The Sarbanes-Oxley Act of 2002 (SOX) requires that management of publicly-traded companies strengthen their processes for assessing and reporting on the internal control over financial reporting. The passage of SOX served as an impetus for the Federal government to re-evaluate its current policies relating to internal control over financial reporting and management's related responsibilities[3]. While SOX created a new requirement for managers of publicly-traded companies to report on the internal control over financial reporting, Federal managers have been subject to internal control reporting requirements for many years. Major Federal internal control related laws and regulations include:

- **The Federal Managers' Financial Integrity Act of 1982 (FMFIA) (Pub, L. No. 97-255) and OMB Circular A-123** requires agencies to establish and maintain internal control. The agency head must annually evaluate and report on the control and financial systems that protect the integrity of Federal programs. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations. The recent revisions to OMB A-123 included the addition of Appendix A, which requires a specific documentation and evaluation methodology for assessing internal controls over financial reporting.

- **The Chief Financial Officers Act of 1990 (CFO Act) (Pub, L. No. 101-576)** requires agency CFOs to develop and maintain an integrated agency accounting and financial management system, including financial reporting and internal controls, which complies with applicable internal control standards.

- **The Government Management Reform Act of 1994 (GMRA) (Pub, L. No. 103-356)** expanded the CFO Act by establishing requirements for the preparation of and audit of agency wide financial statements and consolidated financial statements for the Federal Government as a whole.

- **The Federal Financial Management Improvement Act of 1996 (FFMIA) (Pub, L. No. 104-208)** and **OMB Circular No. A-127 Financial Management Systems** instructs agencies to maintain an integrated financial management system that complies with Federal system requirements, Federal Accounting Standard Advisory Board Standards (FASAB), and the U.S. Standard General Ledger (USSGL) at the transaction level.

- **The Inspector General Act of 1978 (IG Act) (Pub, L. No. 95-452),** as amended, requires that IGs submit semiannual reports to the Congress on significant abuses and deficiencies identified during these reviews and the recommended actions to correct those deficiencies.

- **The GAO Government Auditing Standards (Yellow Book)** and **OMB Bulletin No. 01-02, Audit Requirements for Federal Financial Statements**, as amended, requires auditors to test and report on internal control as part of a Federal agency financial statement audit, including a description of reportable conditions and material weaknesses in internal control over financial reporting.

[3] OMB Circular A-123, pg 20

- **The Government Performance and Results Act (GPRA) (Pub, L. No. 103-62)** promotes results-oriented managing by requiring agencies to develop strategic plans, set performance goals, and report annually on actual performance compared to goals.

- **The Federal Information Security Management Act of 2002 (FISMA) (Pub, L. No. 107-347)** provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. Agencies are required to provide information security controls proportionate with the risk and potential harm of not having those controls in place.

- **The Improper Payments Information Act of 2002 (IPIA) (Pub, L. No. 107-300)** requires agencies to review and identify programs and activities that may be susceptible to significant improper payments. Agencies must annually submit estimates of improper payments, corrective actions to reduce the improper payments, and statements as to whether its current information systems and infrastructure can support the effort to reduce improper payments.

- **The Clinger-Cohen Act of 1996 (Pub, L. No. 104-106)** requires agencies to use a disciplined capital planning and investment control process to maximize the value of and assess and manage the risks of the information technology acquisitions. The Department's policy for management of information resources is contained in Management Directive 1400 Investment Review Process.

1.4 – Standards for Internal Control in the Federal Government

In 1999, the GAO adopted the Committee on Sponsoring Organizations (COSO) framework to define Standards for Internal Control in the Federal Government, i.e., the "Green Book." Internal control is an integral Component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations;

- Reliability of financial reporting; and

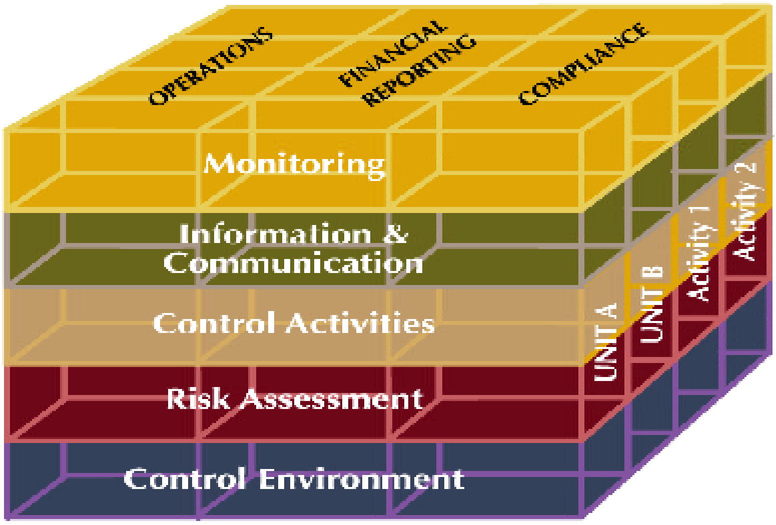
- Compliance with applicable laws and regulations.

Overlaps exist with each internal control objective listed above, however, this guide provides an assessment process as it relates to financial reporting and compliance with laws and regulations that have a direct and material effect on financial reporting. The safeguarding of assets is a subset of all of these objectives. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use or disposition of assets.

Management is responsible for developing and maintaining internal control activities that comply with the following Standards for Internal Control in the Federal Government (referred to as the five standards of internal control or the COSO framework) to meet the above objectives[4]:

[4] OMB Circular A-123, pg 7-8

Figure 3: Standards for Internal Control in the Federal Government



- **Control Environment** – The control environment is the organizational structure and culture created by management and employees to sustain organizational support for effective internal control. The control environment is often called "tone at the top" and is critical to the success or failure of all the other pieces of the internal control framework.

- **Risk Assessment** – Management should identify internal and external risks that may prevent the organization from meeting its objectives. The risk assessment forms the base for all other control activities.

- **Control Activities** – Controls activities include policies, procedures and mechanisms in place to help ensure that agency objectives are met. Control activities, both manual and automated, are the day-to-day controls that form the core of internal controls.

- **Information and Communication** – Relevant, reliable, and timely information should be communicated to relevant personnel at all levels within an organization. Information and communication ensures the internal controls are flexible enough to respond to changes in the control environment on an ongoing basis.

- **Monitoring** – Monitoring the effectiveness of internal control should occur in the normal course of business. Periodic reviews, reconciliations or comparison of data should be included as part of the regular assigned duties of personnel. Monitoring is the process that ensures the control structure is operating as planned and fills all remaining gaps that may exist in the internal control structure.

1.5 – Objectives of Internal Control over Financial Reporting

Point of Focus 1

Effective internal control over financial reporting provides reasonable assurance that misstatements, losses, or noncompliance with applicable laws and regulations, material in relation to financial reports, would be prevented or detected[5].

Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting. It starts at the initiation of a transaction and ends with the reporting. Therefore, internal controls over the transaction process involve controls at every step of the process including the controls over transaction initiation, maintenance of records, the recording of transactions, and final reporting. In addition, it also includes the prevention/detection of unauthorized acquisition, use, or disposition of the agency's assets in relation to the transaction.

Reliability of financial reporting means that management can reasonably make the following assertions[6]:

- The financial report is presented in the proper form and any required disclosures are present (presentation and disclosure) (PD);
- All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date (existence and occurrence) (EO);
- All assets are legally owned by the agency and all liabilities are legal obligations of the agency (rights and obligations) (RO);
- All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (completeness) (CO);
- All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation) (VA);

In addition to the above assertions, OMB Circular A-123 establishes the following assertions as it relates to reliability of financial reporting:

- The transactions are in compliance with applicable laws and regulations (LR);
- All assets have been safeguarded against fraud and abuse; and
- Documentation of internal control, all transactions, and other significant events is readily available for examination.

Defining the Department's internal controls in terms of these objectives will be the basis to support the Secretary's statement of assurance for internal control over financial reporting included as a subset to section 2 of FMFIA reporting.

[5] Derived from GAO/PCIE, Financial Audit Manual, section 310-Overview, Internal Control Phase.
[6] OMB Circular A-123, pg 22

To meet the assertions listed above, controls may be designed to meet certain information processing objectives. These information processing objectives relate to the transactions being processed. At the transaction level, the information processing objectives are categorized into four areas:

- Completeness (C): All transactions that occurred are entered and accepted for processing;
- Accuracy (A): Transactions are recorded at the correct amount, in the appropriate account, on a timely basis (in the proper period);
- Validity (V): All recorded transactions actually occurred (are real), relate to the organization, and were approved by designated personnel;
- Restricted Access (R): Data is protected against unauthorized amendments, its confidentiality is ensured, and physical assets are protected.

1.6 – Revision to OMB Circular A-123 and Appendix A

OMB Circular No. A-123 confirms management's responsibility for internal control in Federal agencies. The Circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control. Appendix A of the Circular provides a methodology to assess internal control over financial reporting and details management's responsibility for the following:

- **Establishment of a Senior Assessment Team**. The Circular requires the establishment of a senior assessment team that includes senior executives and derives its authority and support from the head of the agency or the Chief Financial Officer. The senior assessment team is responsible for oversight over the assessment process. Establishment of the Senior Assessment Team is addressed in Section 2.1 of this guide.
- **Evaluation of Internal Control at the Entity-Level**. The Circular requires the evaluation of the five Components of internal control that have an overarching or pervasive effect on the agency. The five Components of internal control are covered in Appendix P, and internal control at the entity-level is covered in Section 3.2
- **Evaluation of Internal Control at the Process Level**. The Circular requires the identification and evaluation, including assessment of the design and operating effectiveness of the controls, at the account, disclos ure, and related processes level (including transactions and systems). Section 3.4 addresses internal control at this level.
- **Documentation of the Controls and Assessment of Effectiveness**. The Circular requires the documentation of the agency's internal control over financial reporting and documentation of test of controls, identified deficiencies, and assessment of controls at the entity and process level. Documentation requirements are covered in further detail in Section 4, Testing requirements are covered in Section 5, and evaluation of identified deficiencies are covered in Section 6 of this guide.
- **Reporting of Management's Assurance in the PAR**. The Circular requires Agency's management to include an assurance statement on internal control over financial reporting in its annual PAR. Reporting requirements are covered in Section 7.
- **Correction of Material Weaknesses in Internal Control over Financial Reporting.** The Circular requires agencies to establish systems to ensure the prompt and proper resolution and

implementation of corrective action on identified material weaknesses. Section 6.3 addresses remediation of internal control deficiencies and corrective action plans.

1.7. – Key Terms, Definitions, and Acronyms

This guide uses many key terms, definitions and acronyms when discussing the assessment process. For those who may not have had much prior exposure to the concepts and information presented, these terms may initially prove challenging. To aid the user, the most important and common terms and acronyms used throughout the guide are noted in Appendix D – Index of Definitions and Key Terms and Appendix E – Glossary of Acronyms. Successful implementation of this guidance rests upon effective communication. Therefore, users of this guide should thoroughly familiarize themselves with these terms and be able to communicate effectively using them.

SECTION TWO: Project Initiation

Purpose and Scope

This Section identifies the parties charged with project oversight, the Department's Functional Integration Effort, and project management. Undertaking a process to ensure compliance with the internal control provisions of the DHS Financial Accountability Act and the revisions to OMB Circular A-123, Appendix A is a function of the Office of the Chief Financial Officer (OCFO). However, the scope of the assessment will extend well beyond the Department's OCFO into all aspects of the Department's Under Secretary for Management Organization, including the:

- Office of the Chief Information Officer (its OCIO),
- Office of the Chief Administrative Services Officer (OCASO),
- Office of the Chief Human Capital Officer (OCHCO),
- Office of the Chief Procurement Officer (OCPO), and
- Office of the General Counsel (OGC).

As a result, the Department's financial management community will have to coordinate extensively with numerous cross-functional offices, auditors and contractors. While the task will be larger in the initial years, the Department will have to comply annually.

2.1 – Project Oversight

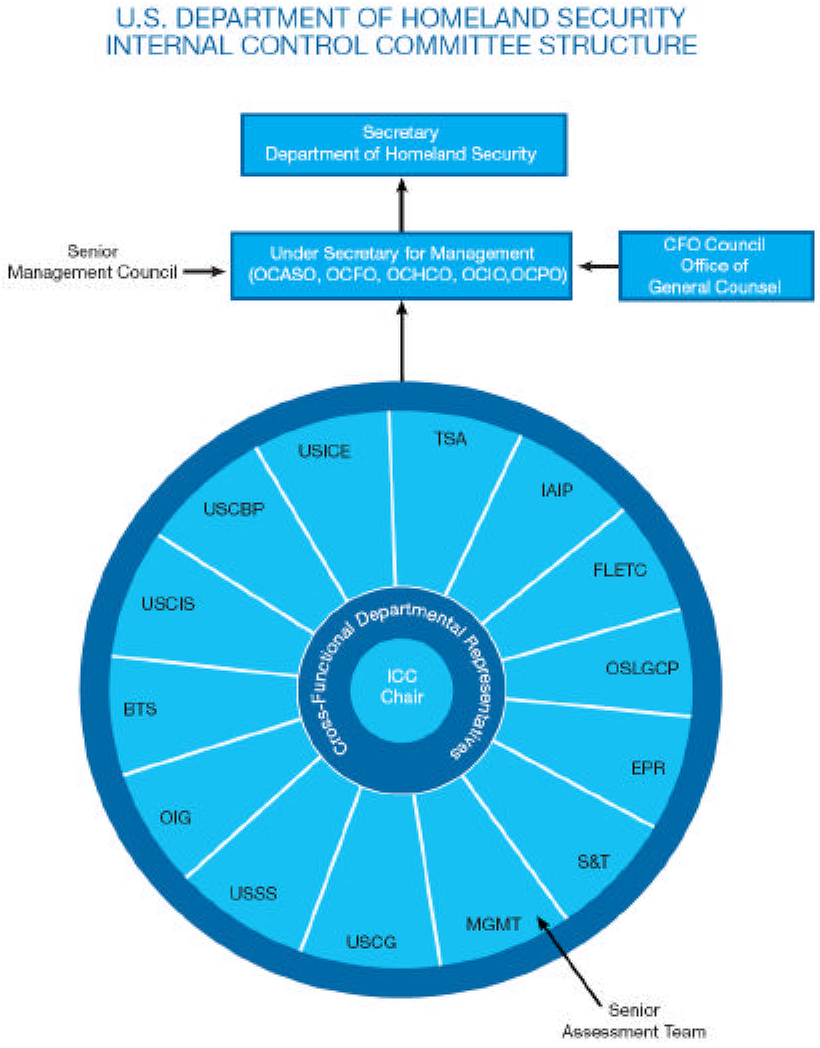
The DHS Financial Accountability Act effort requires broad, senior-level oversight. Establishing accountability for every facet of the project and in every Component and function involved will help make the effort a success. Executive commitment and sponsorship are imperative for the following reasons:

- By its very nature, the project will impact many of the Department's major Components and functions. Typically, the only common leaders of our Components include an Under Secretary, Commandant, Director, Administrator, Commissioner, or Assistant Secretary.
- Some employees might otherwise perceive the compliance effort as concerning primarily the Financial Management Line of Business.
- Completion of the project will require a significant amount of time and resources.

Senior management clearly has a stake in the effort, since the Secretary will be required to provide an assertion on internal control over financial reporting. The key is to ensure that accountability for the project cascades down to all Components. As it would in any high visibility project, senior management should clearly communicate its commitment as frequently as possible, including directly to the Department's personnel or management teams, in intradepartmental newsletters, and in agendas for management meetings. Leadership's commitment must be sustained and continuous. Sustainability of the Department's efforts to achieve effective internal control over financial reporting is important. Compliance with the DHS Financial Accountability Act is much more than a one-time goal; it is a process that must be embedded in the Department.

OMB Circular A-123 recommends establishing a Senior Management Council "to ensure senior management involvement and address management accountability and related issues within the broader context of agency operations." OMB also recommends establishing a Senior Assessment Team to direct the assessment process prescribed in Appendix A. In some cases, Senior Assessment Teams can be supported by contractors. In March of 2005, the Department established an Internal Control Committee (ICC). The ICC has overall responsibility for the effort's successful execution under the leadership of an ICC Board. The ICC Board includes representation from each key stakeholder group, including the cross-functional areas internal to the OCFO and cross-functional areas external to the OCFO, including the OCIO, OCASO, CHCO, OCPO, and OGC. Since the Department is comprised of numerous and complex Components with operations spanning the nation, Components must develop assessment teams within their units. Component Assessment Teams should follow the Department's structure, whether delineated by business unit or geography. The structure of the Department's ICC is depicted in the graphic below:

Figure 4: DHS Internal Control Committee (ICC) Structure


U.S. DEPARTMENT OF HOMELAND SECURITY
INTERNAL CONTROL COMMITTEE STRUCTURE
Secretary
Department of Homeland Security
Senior
Management Council
Under Secretary for Management
(OCASO, OCFO, OCHCO, OCIO,OCPO)
CFO Council
Office of
General Counsel
TSA
IAIP
FLETC
OSLGCP
EPR
S&T
MGMT
USCG
USSS
OIG
BTS
USCIS
USCBP
USICE
Cross-Functional Departmental Representatives
ICC
Chair
Senior
Assessment Team

See Appendix C for the ICC Charter, which details the specific oversight, responsibilities, structure, and management of the ICC.

2.2 – Line of Business Integration and Management

In August 2004, Secretary Ridge initiated the Department's Functional Integration Effort "to involve all the functional experts under one integrated method of operation." The Secretary's vision for the functional integration effort included:

- Creation of systems and processes that create seamless efforts whereby the Federal Government is responsive to the needs of every citizen;
- Integrated methods of operation amongst and between the various operational entities of the Department;
- Support systems enhance mission effectiveness and create economies of scale through the consolidation of high volume transaction centers (including shared services); and
- Properly placed accountability on DHS leadership to be aggressively responsible for the actual integration effort. This involves a concept of dual accountability where both the operational leadership (agency heads and line directors) and the support structure leadership (Line of Business Chiefs) are responsible for implementation.

The Secretary's vision resulted in the series of Management Directives listed below.

- Acquisition Line of Business Integration and Management (MD No. 0003)
- Administrative Services Line of Business Integration and Management (MD No. 0004)
- Financial Management Line of Business Integration and Management (MD No. 0005)
- Human Capital Line of Business Integration and Management (MD No. 0006); and
- Information Technology Integration and Management (MD No. 0007).

These Management Directives are the principle documents for leading, governing, integrating, and managing various functions throughout the Department. The Department plans to use these management directives to establish accountability for internal controls at the Department.

Accountability starts with the executive sponsor of the program (e.g., the Department's Senior Management Council). It is then delegated among various lines of business throughout the Department. Regardless of who documents an organization's processes and controls or who performs the testing for operational effectiveness, the lines of business in charge of a particular process must take responsibility and ownership for processes and controls, ensuring that the control objectives are met. As management determines who is responsible for documenting and testing controls, it must evaluate the competence and objectivity of the individuals to ensure that sufficient assurance is obtained from the procedures performed.

As the Department has encountered in its initial start up years, there is ambiguity about who is ultimately responsible for a process from beginning to end. Often, operational management believes that the OCFO is solely responsible for the financial reporting process. While this is true for certain processes, such as period-end financial reporting, much of the information in the financial statements originates outside the financial management line of business of the Department. While the Department's OCFO may establish many of the policies for maintaining the integrity of financial reporting, the procedures and controls for complying with these policies are largely overseen by other CXOs. Examples of cross functional involvement include:

- OCIO: The OCIO will have two primary roles in the project: First, to document and self-assess its own significant processes (referred to as general computer controls) for (a) the information technology control environment, (b) the development and implementation of information technology (program development), (c) a change to existing information technology (program changes), (d) information security (access to programs and data), and (e) computer operations. These are pervasive controls since the effectiveness of all automated controls across the organization depends on them. Second, to support personnel who are responsible for specific processes by helping those individuals document and assess their control activities. Because those individuals are accountable for the controls pertaining to the processes they oversee, they should be responsible for documenting and testing both manual and automated controls, even though automated controls often rely on or reside in information technology systems. It is important for personnel who are responsible for processes in their business units to understand all the controls for their processes, not simply the manual controls.

- OCPO: The OCPO's role will include responsibility for internal controls over acquisition and grants management processes that overlap financial management processes within the Department. For example, per section 2.101 of the Federal Acquisition Regulation, "acquisition means the acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract." Grants management includes the process of issuing and managing assistance awards, e.g. grant awards, cooperative agreements, and other types of assistance, between the Department and non-Federal entities, e.g. State , local and Tribal governments, non-profit organizations, profit companies, or individuals to address a public need. Assistance awards are legal agreements that typically specify periods of performance, scope of work, budget, and terms and conditions.

- OCHCO: The OCHCO's MAXHR program will provide the framework to establish Components of the control environment related to commitment to competence, for example, identifying knowledge skills, and abilities, counseling policies to improve performance, etc. Establishment and development of MAXHR will ensure the Department can continue to attract, retain, and reward a workforce that is able to meet the Department's critical mission.

- OGC: The OGC's role will include providing expert legal advice to identify significant provisions of laws and regulations that have a direct and material effect on determining amounts in the financial statements, controls over compliance with laws and regulations, and identification of contingencies for disclosure and accrual. In addition, the Legal Advisor for Ethics will establish the control environment as it relates to integrity and ethical values.

- OCASO: The OCASO's role will include responsibility for internal controls over asset management processes that overlap financial management processes within the Department. For example, ensuring all assets have been safeguarded against fraud and abuse. The safeguarding of assets is a subset of all three objectives of internal control; therefore, the role of the OCAS will be invaluable to establish procedures, processes, and policies that reduce vulnerabilities and minimize asset management risks.

2.3 – Project Management

A well-established framework for governing compliance with the DHS Financial Accountability Act will not, in itself, guarantee success. The project's success will also depend on strong execution, which in turn will largely depend on disciplined management of the project. Implementing the DHS Financial Accountability Act will require full-time project management with a focus on the tools and methodologies associated with this discipline (i.e., developing and maintaining formal project plans, facilitating regular status meetings, and using a set of defined metrics to ensure rigor in the reporting to management). For a large, complex, multi-Component Department, Component level assessment teams will be required at each material Component. Smaller Component level assessment teams may be established for Components serviced by others. Individuals assigned to Component level assessment team should have full-time responsibility for the effort. It will be very difficult to manage the challenges of the DHS Financial Accountability Act on an "other duties as assigned basis" or part-time schedule. Although Component level assessment teams may be assigned for the initial years of compliance, ultimately, Components should integrate compliance into their day-to-day operations.

Some may regard the creation of separate teams to manage compliance with the DHS Financial Accountability Act as resulting in unnecessary overhead, but the Department will be required to coordinate numerous teams, which will document hundreds of control activities, and confront possibly hundreds of internal control deficiencies, many of which will require remediation. Without dedicated personnel with expertise in project management, the DHS Financial Accountability Act project quickly can become overwhelming. Project management helps to:

- Establish and manage accountability across organizational units;
- Ensure attainment of deadlines;
- Develop consistent standards for documentation, testing, and reporting across organizational units;
- Provide a mechanism to react to remediation requirements; and
- Provide a communication channel.

Because no Department is static, documentation and testing will need to be updated prior to the reporting date. Therefore, key to managing the DHS Financial Accountability Act project is establishing an infrastructure and methodology for tracking and incorporating changes in internal control to ensure that the controls documented and tested by management represent those in effect as of the year-end date. Otherwise, management may inadvertently fail to test controls that have changed since its original assessment, which increases the risk that an internal control deficiency may exist but not be discovered or be discovered too late in the year for remediation prior to the reporting date.

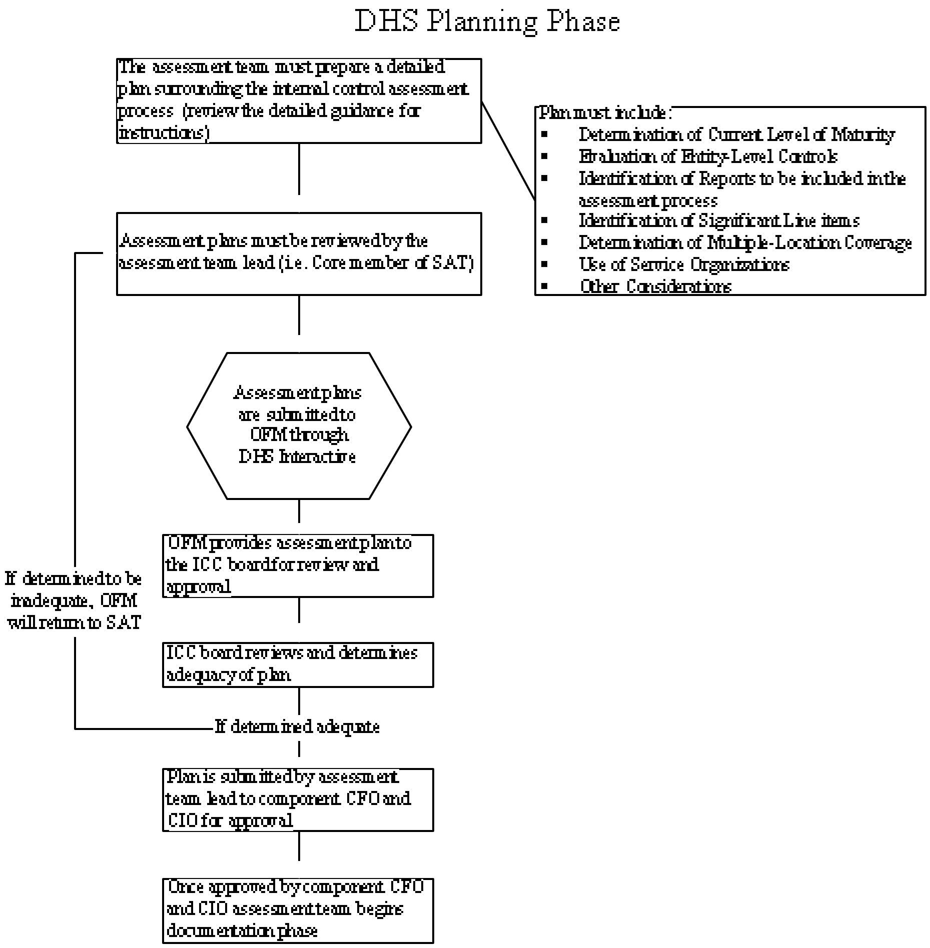
As the Department's efforts to comply with the DHS Financial Accountability Act mature, the OCFO will evaluate the structure of assessment teams annually.

SECTION THREE: Planning Phase

Purpose and Scope

The Planning Phase involves a top down approach to determine the documentation necessary and the nature, timing, and extent of testing of controls to be performed for each significant line item and related account, disclosure, and process (including related transactions and systems) at each of the organization's locations. OMB Circular A-123, Appendix A requires that the assessment be carried out in a thorough, effective, and timely manner.[7] At each of the Department's Components, the responsibility for planning falls under the Component Assessment Team (refer to as the "assessment team") headed by a core member of the Senior Assessment Team. This assessment team will conduct planning for the entire Component. Planning is one of the most critical phases in management's assessment. During this phase, the assessment team must identify the significant line items and related accounts, disclosures, and organizational processes/cycles and sub-processes/sub-cycles; and locations that will be subject to procedures.

Figure 5: Overview: The Planning Phase


DHS Planning Phase
The assessment team must prepare a detailed plan surrounding the internal control assessment process (review the detailed guidance for instructions)
Plan must include:
▪ Determination of Current Level of Maturity
▪ Evaluation of Entity-Level Controls
▪ Identification of Reports to be included in the assessment process
▪ Identification of Significant Line items
▪ Determination of Multiple-Location Coverage
▪ Use of Service Organizations
▪ Other Considerations
Assessment plans must be reviewed by the assessment team lead (i.e. Core member of SAT)
Assessment plans are submitted to OFM through DHS Interactive
OFM provides assessment plan to the ICC board for review and approval
If determined to be inadequate, OFM will return to SAT
ICC board reviews and determines adequacy of plan
If determined adequate
Plan is submitted by assessment team lead to component CFO and CIO for approval
Once approved by component CFO and CIO assessment team begins documentation phase

This section provides an overview of how the assessment team should identify its significant line items and related accounts, disclosures, processes/cycles (including related transactions and systems), and locations that are subject to assessment. Then, specific planning considerations are addressed as they relate to the five standards of internal control, (1) control environment, (2) risk assessment, (3) control activities, (4) information and communications, and (5) monitoring. Finally, the period-end reporting process, accounting estimates and judgments, application controls, general computer controls, compliance with laws and regulations, mergers/consolidations, new systems, and use of service organizations warrant specific discussion and are covered later in this section.

[7] OMB Circular A-123 Management Responsibility for Internal Control, Appendix A, page 24.

Significant judgment is involved in planning decisions because of the complexity of the Department's organizational structure. The assessment team must maintain documentation to support each key decision.

Although the objective of the planning phase is to identify the significant line items and related accounts, disclosures, processes/cycles (including related transactions and systems), and locations that must be documented and tested, many different approaches may be taken to get to this end result. Although the planning phase is presented as a sequence of steps, they are inter-related and should be performed simultaneously. The assessment team may identify significant line items and map these line items to the processes/cycles; alternatively, management may begin the process by identifying the processes/cycles. Regardless of the approach taken, the ultimate objective of the exercise is the same.

The assessment team must prepare a detail plan surrounding their internal control assessment approach (Refer to planning steps below). The assessment plan must be reviewed by the assessment team lead. Assessment plans must be submitted to OFM electronically via the Department's intranet site at https://interactive.dhs.gov, within the specified timeframe. OFM will provide the Components' plan to the ICC board for approval. If the ICC board finds the plan to be inadequate, OFM will notify the assessment team lead. The notification will include areas for improvement or where clarification is needed. The assessment team must re-submit the plan within the deadlines established by OFM. Once approved by the Component CFO and CIO, the assessment team may begin the next phase of the assessment. The ICC will determine the plan at the Department Level.

To meet its responsibility, the assessment team must follow the following steps when performing the planning phase of the assessment:

- Step 1: Identify Maturity Level of Internal Control Over Financial Reporting
- Step 2: Assess Entity Level Controls
- Step 3: Identify Reports to be included in the Assessment of Financial Reporting
- Step 4: Identify Significant Line items and Related Accounts, Disclosures and Process /Cycles
    - Step 4a: Identify significant line items and related accounts and disclosures by considering materiality and separately disclosed items
    - Step 4b: Identify processes/cycles and sub-processes/cycles and map to significant line item and related accounts and disclosures
    - Step 4c: Identify the relevant financial statement assertions for each significant line item and related account and disclosure
    - Step 4d: Perform a risk assessment of the sub-processes/sub-cycles
- Step 5: Determine Multiple-Location Coverage
- Step 6: Other Considerations
    - Step 6a: Period End Financial Process
    - Step 6b: Accounting Estimates and Judgments
    - Step 6c: Control Activities Specific for Information Systems
    - Step 6d: Compliance with Laws and Regulations

Step 6e:Mergers/Consolidations

Step 6f: New Systems (e.g. eMerge)

Step 7: Use of Service Organizations

Step 7a: Determine if a service organization is being used

Step 7b: Determine of the outsourced activities, processes, and functions are significant to the entity internal control over financial reporting

Step 7c: Determine if an Annual Assurance Statement (cross-servicing organization) or a SAS 70 (commercial company) exists and is sufficient in scope

Step 7d:If an Annual Assurance Statement or SAS 70 does not exist, determine alternative procedures

Point of Focus 2

External Auditor Interaction

To facilitate an open dialogue and timely identification and resolution of issues, participation by the external auditor is encouraged. The external auditor can also provide input on any new interpretive guidance issued by the staffs of the AICPA, GAO, or PCAOB.

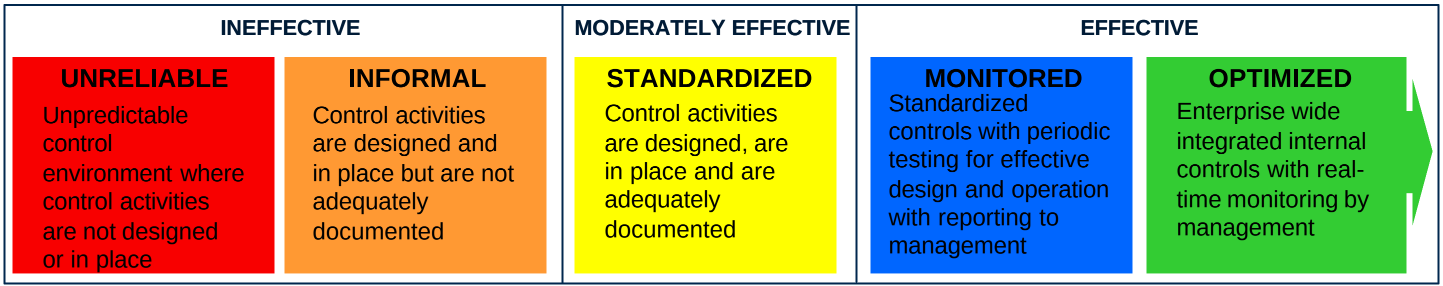
3.1 – Step 1: Identify the Maturity Level of Internal Control over Financial Reporting

Management should have a vision for internal control throughout the organization that includes:

1. Identification of the current effectiveness of internal control based on documentation and tested results,
2. The short-term (annual) desired effectiveness of internal control with an action plan, and
3. The long-term desired effectiveness of internal control with a long-term action plan.

A Maturity Model illustrates the five maturity levels of internal control over financial reporting in an entity.

Figure 6: The Maturity Level of Internal Control over Financial Reporting



INEFFECTIVE

UNRELIABLE Unpredictable control environment where control activities are not designed or in place

INFORMAL Control activities are designed and in place but are not adequately documented

MODERATELY EFFECTIVE

STANDARDIZED Control activities are designed, are in place and are adequately documented

EFFECTIVE

MONITORED Standardized controls with periodic testing for effective design and operation with reporting to management

OPTIMIZED Enterprise wide integrated internal controls with real-time monitoring by management

[8]©PricewaterhouseCoopers all rights reserved.

Determining an operating unit's maturity level over financial reporting will help determine where to start. Some may want to "dive into documenting, evaluating, testing, and remediating" control weaknesses; however, using a maturity model will help us plan our assessment "in a thoughtful way."[9] The ICC Board and Senior Assessment Team should be able to determine the current maturity based off of results of previous year's testing, auditor reports, IG reports, existing documentation, self assessments, and other data. Once the current maturity is identified a goal for improvement should be set for the next fiscal year. To meet that goal and have it reflected in the PAR, management must implement relevant changes during the first two quarters of the year. The remainder of the year will be necessary for self-assessment testing and remediating identified deficiencies. The short-term goal should never overshadow the long-term vision. The Department is committed to integrating optimized internal controls into the agency.

The determination of current maturity of Internal Control over Financial Reporting should be documented by the assessment team at the Component level and by the ICC board at the Department level. The assessment teams should support their determinations by identifying the basis for the determination (i.e. results of previous year's testing, auditor reports, IG reports, existing documentation, self-assessments, and other data).

Improving internal control is a function of two factors:

1. The confidence placed on controls (i.e., their actual effectiveness); and
2. The efficiency with which they are performed (i.e., part of regular operation or separate tedious exercise).

[8] PricewaterhouseCoopers LLP Maturity Model©

[9] Deloitte, Taking Control – A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002.

Figure 7: Internal Control Certification Effort

Low Confidence

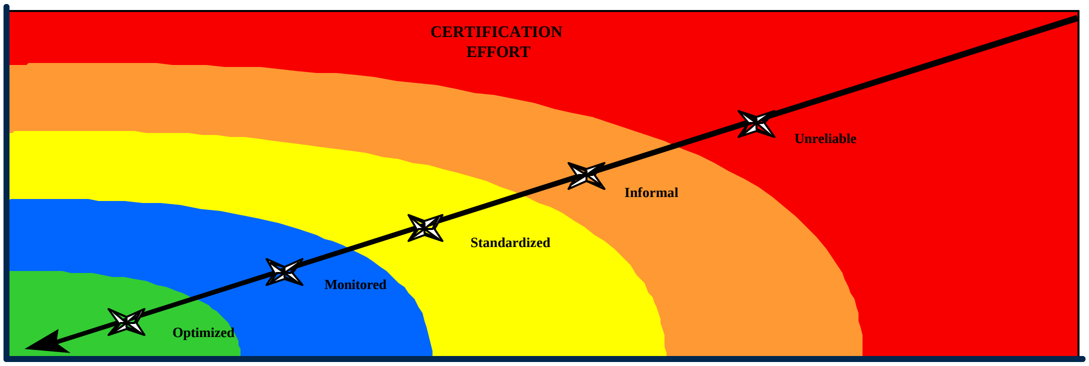
Controls not in place or poorly documented and communicated. Little or no monitoring and testing.

Medium Confidence

Documented and communicated. Some monitoring in place. Little or no testing.

High Confidence

Documented and communicated. Monitored and tested. Functioning as intended.



High Efficiency

- Reliance on continual monitoring and review of periodic testing
- Use of a uniform dashboard for key indicators & controls
- Reliance on certifications and acknowledgements
- Mgt. Time Commitment: Moderate

Medium Efficiency

- Manual testing required for key activities once a year
- reliance on annual monitoring and documentation
- Reliance on certifications and acknowledgements
- Mgt. Time Commitment: High

Low Efficiency

- Substantial manual efforts
- Testing and validation required of activities
- Mgt. Time Commitment: Very High

[10]©PricewaterhouseCoopers all rights reserved.

Management may be confident that internal control is effective, but still suffers unnecessary inefficiency in operation. Likewise, management may incorporate an efficient internal control structure, but fail to achieve the desired confidence in design and operating effectiveness. Because a key Component of the goal for internal control is to achieve an optimal cost/benefit relationship, the combination of confidence and efficiency is where controls become truly optimized.

3.2 – Step 2: Assess Entity-Level Controls

Entity level controls start with the five elements of internal control discussed in Section 1.4 (i.e. Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring). It also includes other controls that are pervasive in nature and that the entity has determined to be necessary in order to carry out their operations. These controls provide additional assurance that appropriate controls are operating throughout the organization and are especially important when an organization has multiple locations/operating units (the terms location(s) and operating unit(s) are used interchangeably in this document, refer to Appendix D - Index of Definitions and Key Terms) which perform similar types of functions. For example, immigration offices across the country should have uniform procedures and controls in place to ensure the secure and accurate receipt and recording of fees. Part of the control structure is ensuring that each immigration office follows the entity-level controls.

As part of the assessment, the assessment team must document, test, and evaluate the design and effectiveness of the five standards of internal control (and other entity-level controls). Because these controls form the foundation for all other controls implemented within an organization, it is important to document these controls during the planning phase of the assessment. Testing and evaluating these controls may be completed as part of the planning phase or during the very early stages of the testing phase. However, it is recommended that the testing and evaluation of these foundation controls occur as early in the assessment phase as possible. Many deficiencies in entity-level controls may also require several months to remediate. Inadequate entity-level controls may be an indicator that the control environment is ineffective. Weaknesses

[10] PricewaterhouseCoopers LLP Maturity Model©

or deficiencies noted within these foundation controls will need to be remediated as soon as possible to prevent the weakening of other internal controls.

Entity-level controls should also be considered at individually important locations (refer to Section 3.5 for discussion of multi-location coverage). Management's evaluation of entity-level controls will impact the nature, timing, and extent of tests of controls at individually important locations.

The assessment team should consider where in the organization the entity-level controls operate (i.e., Department level, Component level, location/operating unit-level, or a process level). Although the Department/Component level may be responsible for compiling and issuing an accounting policies and procedures manual, the assessment team must perform testing at the individual locations to ensure that the policies are being appropriately applied. Appendix P describes in more detail the five Components of internal control and factors that the assessment team should consider when documenting, testing and evaluating these Components and the level where it should be documented. Additional testing guidelines are provided within the testing section.

Figure 8: Entity-Level Controls

Examples of Entity-Level Controls*										
Components of Internal Control and Anti-Fraud Programs	Human Resources	Inspector General	Whistleblower	Code of Conduct	Information Technology Environment & Organization	Self-Assessment	Operational/Program Controls	Policies and Procedures Manual	Period-End Reporting	Performance Reviews
Anti-Fraud Program	X	X	X	X					X	
Control Environment	X		X	X	X			X		
Risk Assessment	X	X	X			X				
Control Activities							X		X	X
Information & Communication	X	X	X	X	X		X	X	X	
Monitoring		X	X			X		X		

*The "X's" represent examples of areas within the five Components of internal control and an organization's anti-fraud program where entity-level controls are evidenced. As mentioned in Appendix P, the Senior

Assessment Team must address the organization's anti-fraud program when evaluating the control environment.

3.3 – Step 3: Identify Reports to be Included in the Assessment of 'Financial Reporting'

The assessment teams are responsible for identifying which financial reports are deemed to be 'significant' and therefore subject to the internal control assessment. Key decisions must be documented thoroughly and readily available for review by members of the Senior Assessment Team and the ICC board, OMB and external auditor. At a minimum, reports which are deemed significant are[11]:

- Annual Financial Statements:
  - Consolidated Balance Sheet,
  - Consolidated Statement of Net Cost,
  - Consolidated Statement of Changes in Net Position,
  - Combined Statement of Budgetary Resources,
  - Consolidated Statement of Financing,
  - Statement of Custodial Activity, and
  - Notes to the Consolidated Financial Statements,
- Quarterly Financial Statements:
  - Consolidated Balance Sheet,
  - Consolidated Statement of Net Cost, and
  - Combined Statement of Budgetary Resources.

Additionally, any financial reports that could have a material effect on a significant spending, budgetary or other financial decision of the organization, or that is used to determine compliance with laws and regulations (having a direct effect on the financial statements) on the part of the organization. Other reports to consider include[12]:

- SF-133 *Report on Budget Execution and Budgetary Resources*;
- FMS 2108 *Yearend Closing Statement;*
- SF-132 *Apportionment and Reapportionment Schedule;*
- President's Program and Finance Schedules;

[11] OMB Circular A-123, pg 22

[12] OMB Circular A-123, pg 22

- Budget Submissions;
- Required Supplementary Information (RSI);
- Required Supplementary Stewardship Information (RSSI);
- Governmentwide Financial Reporting System (GFRS);
- Account Trial Balance (ATB) Reports;
- SF-224 Statement of Transactions;
- Financial Information included in the Department's Management Discussion and Analysis section of the PAR, specifically the Financial Highlights;
- Reports used to monitor specific activities such as specific revenues, receivables, or liabilities; and
- Reports used to monitor compliance with laws and regulations such as the Anti-Deficiency Act.

After determining which financial reports should be covered within the assessment, a series of steps will be completed by the assessment team to identify the risks and controls associated with each report. These steps will be discussed in further detail within this section of the guide. For ease of reference, the following sections refer to the consolidated financial statements. As noted, these steps would be completed for each of the significant financial reports.

3.4 – Step 4: Identify Significant Line items and Related Accounts, Disclosures, and Processes/Cycles (including related transactions and systems)

One objective of the project is to determine the controls that address the relevant financial statement assertions for each significant line item and related account and disclosure in the external financial reports. To accomplish this objective, the assessment team should start with the consolidated financial statements and footnotes, and then move through each step, ultimately determining the internal control activities and procedures that address the relevant financial statement assertions. The steps to identify the significant accounts, processes, and sub-processes; and how to link those to management's assertions are further explained below.

Step 4a: Identify significant line items and related accounts and disclosures by considering

- Items separately disclosed in the organization's consolidated financial statements; and
- Materiality, both quantitative and qualitative factors.

Items separately disclosed in the organization's consolidated financial statements

Significant accounts and disclosures are identified at the (1) organization's consolidated financial statement level and (2) individual line item/Component or disclosure level (e.g., revenue may comprise exchange revenue and non-exchange revenue). A line item or disclosure should be considered significant if individually or when aggregated with other misstatements, could have a material effect on the financial statements as a result of either overstatement or understatement[13]. The notion of "significance" should not be based solely on a quantitative measure. Certain accounts may be significant on a qualitative basis or because they represent an important performance measure to users.

For purposes of determining significant accounts, the assessment team should assess the likelihood of a misstatement without giving any consideration to the effectiveness of internal control over financial reporting. The accounts and disclosures that are presented in the financial statements and footnotes represent the starting point for determining which accounts are significant. The assessment team should consider the following key points when assessing significance:

- There is a presumption that, taken as a whole, all line items and footnotes (e.g., Fund Balance with Treasury, Accounts Payable, Liabilities not Covered by Budgetary Resources) in the financial statements are significant. However, if the financial statements are highly disaggregated, typically management should presume that all consolidated balance sheet and statement of net cost account balances/Components that are greater than management's design materiality threshold are significant. (Materiality is discussed below)
- Line Items that may not be significant at a particular time but undergo significant activity (e.g., Fund Balance with Treasury) or have exposure to unrecorded obligations (e.g., unfunded liabilities) generally also would be considered significant.

It is important that the assessment team implement a process for regularly reassessing its initial planning phase decisions to ensure that they are appropriately updated for significant organizational changes. Because planning decisions are made early in the process, it is likely that certain aspects of those decisions will change as the year progresses. Factors that may impact planning decisions include:

- Determination of specific risk areas at a location
- Changes in management at an individual location
- Identification of internal control deficiencies

Materiality

Point of Focus 3

<u>Definition of Materiality</u>

"The omission or misstatement of an item in a financial report if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item."[14]

In order to determine which accounts are significant, the assessment team must consider the concept of materiality. The same definition of materiality that applies to the preparation of financial statements applies to planning and reporting the effectiveness of internal control over financial reporting. Materiality is more than just

[13] PCAOB AS2.

[14] Financial Accounting Standards Board (FASB) Statement of Financial Concepts No. 2.

a quantitative concept; judgments about materiality are subjective and may change throughout the process. The assessment team must make its own materiality decisions.

Quantitative Considerations

The concept of materiality is applied to the consolidated financial statements and to individual accounts/Components. From a quantitative perspective, materiality has three Components: a materiality base; planning materiality; and design materiality[15]. The assessment team should determine and document each of these Components of materiality.

Materiality Base: The materiality base is the element of the financial statements or report that is most significant to the primary users of the statements. The materiality base generally should be the greater of total assets or expenses (net of adjustments for intragovernmental balances and offsetting balances). Other materiality bases that might be considered include total liabilities, revenues, and appropriations.

For purposes of calculating materiality, organizations should use their prior fiscal year consolidated financial statements. If significant changes in the balances are expected, then the organization should estimate the year-end balance of the materiality base.

For example, the Department at the consolidated level will choose gross cost as the materiality base. For FY 2004, the DHS gross cost net of intragovernmental activity at the consolidated level was $32,742,000,000.

FY 05 Materiality base = Gross Cost of $32,742,000,000

Planning materiality: Planning materiality is a preliminary estimate of materiality, in relation to the consolidated financial statements. Planning materiality is used to assess whether aggregated misstatements at the level of an individual significant line items (and, similarly, the aggregated deficiencies in an audit of internal control) are material to the consolidated financial statements.

Planning materiality generally should be 3 percent of the materiality base. Although a mechanical means might be used to compute planning materiality, management should use judgment in evaluating whether the computed level is appropriate. The assessment team should consider adjusting the materiality base for the impact of such items as unfunded liabilities, contingencies, and other items that may not be reflected in the materiality base but that may be important to the financial statement user.

Based on the example above, planning materiality for the Department at the consolidated level would be calculated as follows:

FY 05 Planning materiality = Materiality Base of $32,742,000,000 x 3% = $982,260,000

Design materiality: Is the portion of planning materiality that has been allocated to line items and related accounts and disclosures. To provide an allowance for the aggregation of misstatements across individual accounts and for detection risk (the risk that controls will fail to detect a material misstatement), design materiality should be one-third of planning materiality.

Continuing the example above, design/test materiality for the Department would be calculated as follows:

[15] Definitions adapted from the GAO/PCIE Financial Audit Manual, section 230. Please note that materiality, as defined by the FAM, differs from materiality as defined by OMB Circular A-123. The differences are in name only, and not in quantitative measure. Use of FAM methodology is wholly consistent with the Circular.

Design materiality = Planning materiality of $982,260,000 / 3 = $327,420,000

Planning materiality and design materiality levels should be documented, along with (1) the rationale behind the quantitative materiality levels and (2) any changes in the determination of materiality that arise during the remainder of the project.

When identifying significant line items, the assessment team must disaggregate the Components of line items, accounts and related footnote disclosures to determine whether any of the Components are individually significant. For example, the "Other Assets" line item on the consolidated balance sheet may include multiple accounts or classes of transactions which are connected to different risks or controls. In this case, these accounts/Components should be assessed separately. Other examples include:

- Revenue streams having different characteristics (e.g., product revenues versus fee revenues);
- Different Components of inventory (e.g., raw materials, work-in-process, and finished goods); and
- Contract-driven service fees versus expenses for materials and supplies.

If any of these Components exceed the design materiality threshold, it should be considered significant, even though it is not separately disclosed in the financial statements.

Based on the example above, gross cost at each separately disclosed component, except for Information Analysis & Infrastructure Protection and Departmental Operations and Other, would be considered significant.

Information Analysis & Infrastructure Protection -

Gross Cost = $148,000,000 < $327,420,000 (design materiality)

Departmental Operations and Other –

Gross Cost = $192,000,000 < $327,420,000 (design materiality)

Qualitative Considerations

The following examples of qualitative factors also should be considered when assessing the significance of an account[16]:

- Composition of the account (does the account relate to a mission critical aspect of the Component) (e.g., Tax, Duties, and Trade Receivables);
- Susceptibility to loss due to errors or fraud (is the account a key line item);
- Volume of activity, complexity, and homogeneity of the individual transactions processed through the account (e.g., fund balance with treasury);
- Nature of the account (for example, suspense accounts generally warrant greater attention);
- Accounting and reporting complexities associated with the account (does the account contain large estimates or accruals);
- Exposure to losses represented by the account (e.g., contingent liabilities);

[16] Adapted from PCAOB AS2.

- Likelihood (or possibility) of significant contingent liabilities arising from the activities represented by the account (e.g., environmental liability);
- Existence of intragovernmental and intradepartmental transactions in the account (e.g., intragovernmental receivables);
- Changes in account characteristics since the previous period (e.g., new complexities, subjectivity, or types of transactions); and
- Visibility and sensitivity of a program, activity, and function.

The assessment team must calculate materiality based on quantitative and qualitative measures at the Component level. The ICC board will approve materiality consideration along with all other planning considerations made by the assessment teams. The materiality at the Department level will be computed for the Department by OFM and approved by the ICC board.

The assessment team should consider all of the aforementioned factors when deciding whether to include or exclude specified accounts in its assessment.

Step 4b: Identify processes/cycles and sub-processes/cycles and map to significant line item and related accounts and disclosures.

Point of Focus 4

It is beneficial to address the information processing objectives/CAVR (completeness, accuracy, validity, and restricted access) at the transaction level for each process because until the assessment team understands the controls within the processes/cycles that generate the account, it may be difficult for management to determine the effectiveness of controls for an account. By testing a control activity only at the level of the financial statement assertion, management might not determine to its satisfaction that (1) controls are in place for the input, processing, and recording of the data underlying the financial statement Component and (2) the entire control system for that process is in place and functioning as intended.

Next, the assessment team determines the significant processes/cycles and sub-processes/sub-cycles that generate the significant accounts. A process or cycle is any sequence of transactions that enables an entity to complete tasks and achieve its objectives. A sub-process or sub-cycle is a group of transactions for which specific accounting procedures and controls are established by an entity's management. For example, a revenue and receivables process may include sub-processes, such as invoicing, pricing, or processing of receipts. Other examples of common processes/cycles and sub-processes/sub-cycles are provided in Appendix F.

The Component's processes/cycles are the foundation for the internal control assessment. By understanding and documenting the processes/cycles, the assessment team is able to identify the control activities that address the information processing objectives/CAVR, as well as potential "gaps" in the controls (i.e., information processing objectives for which control activities are not in place). Refer to Appendix D for a discussion of information processing objectives/CAVR.

Mapping is an exercise performed to link significant accounts to the processes/cycles or sub-processes/sub-cycles that generate them. Mappings are useful to ensure that all significant accounts have been addressed by a process/cycle and that all significant processes/cycles have been identified. If the assessment team fails to identify all of the processes, it will be more difficult to determine the corresponding control activities that address each relevant assertion. Within each process and sub-process, management determines which control activities address the information processing objectives/CAVR over the significant accounts. Appendix I includes examples of how the significant financial statement line items could be mapped to the cycles.

Point of Focus 5

The assessment team should not only focus on routine/transactional processes and control activities but also focus on accounts that are most susceptible to material misstatement. Often these accounts are not transactional but rather, non-routine accounts that involve significant judgment and estimation (i.e. liability estimates such as benefits payable).

Step 4c: Identify the relevant financial statement assertions for each significant line item and related account and disclosure.

For each significant account and disclosure, the assessment team should identify and document relevant financial statement assertions, as well as test the controls that apply to those assertions (testing will be discussed in Section 5 of this guide). The assertions are:

- existence or occurrence
- completeness
- valuation or allocation
- rights and obligations
- presentation and disclosure
- compliance

Refer to Appendix D for descriptions and examples of each assertion.

Relevant assertions are assertions that have a meaningful bearing on whether the account or disclosure is fairly stated. The degree to which an assertion is relevant to each significant account will vary[17]. For example, assertions about valuation may not be relevant to the accounts receivable account unless there is doubt regarding collectibility; however, assertions about existence and completeness are always relevant. Additionally, the assessment team may focus on assertions about presentation and disclosure separately, in connection with the period-end financial reporting process. In determining whether a particular assertion is relevant, the assessment team should consider:

- The nature of the assertion;
- The volume of transactions or data related to the assertion; and
- The nature and complexity of systems, including information technology systems that the entity uses to process and control information that supports the assertion.

[17] PCAOB AS2.

The assessment team should determine relevant assertions prior to testing to minimize the likelihood of testing controls that address assertions that are not relevant to a particular significant account.

Although the financial statement assertions appear to be similar to the information processing objectives/ CAVR, there is not a one-for-one relationship, and they are used for different purposes. Information processing objectives/CAVR are used to evaluate the design effectiveness of controls, particularly application controls, within a process. Financial statement assertions are representations by management as to the fair presentation of the financial statements.

Step 4d: Perform a risk assessment of the sub-processes/sub-cycles.

The next step in the planning phase is to identify the risks within the sub-processes/sub-cycles that may result in a material misstatement in the financial statements. The risk assessment will be used to assess the nature, timing, and extent of the testing that must be performed in each area. For example, fixed asset balances may be significant; however, the balances are less judgmental in nature and thus are of lower risk. In these cases, testing of the control activities that support the processes around capital expenditures may be performed earlier in the year or the extent of testing may be reduced. The risk assessment requires significant judgment and should be performed by members of the assessment team that have sufficient knowledge of the processes and associated risks. As with the determination of significant accounts, qualitative and quantitative factors must be considered. Various methods may be used to perform the risk assessment. The assessment team should determine its strategy for assessing the risk for each process/cycle and ensure that its methodology is consistently applied and sufficiently documented.

Refer to Appendices I and J for risk assessment instruction and related documentation template.

3.5 – Step 5: Determine Multiple-Location Coverage

In cases where the processes/cycles and sub-processes/sub-cycles take place at multiple locations/operating units within the Department/Components, the assessment team must decide which locations will be included in its internal control assessment. These locations will be referred to as “individually important” or “financially significant” (these terms will be used interchangeably in this document)[18]. In addition to individually important locations, the assessment team will need to perform certain procedures at locations with specific risks and locations that are not individually important, but that may be significant when aggregated with other locations. The general decision tree, figure 9, can be used by the assessment team as a guide through this decision process.

The assessment team must decide which locations or operating units should be included in its assessment by evaluating factors such as:

- the operations of the location/operating unit;
- the risk of material misstatement that the location/operating unit poses; and
- the extent to which processes/cycles and underlying controls for a given location/operating unit are part of a central-processing or shared-services environment.

Ultimately, controls will be identified and tested at the location that is responsible for implementing them. When determining the locations or operating units that are subject to assessment, the assessment team

[18] PCAOB AS2.

should identify all locations. Although this may seem like a straightforward task, it may prove challenging for the Department or its Components because of its complex and diverse missions.

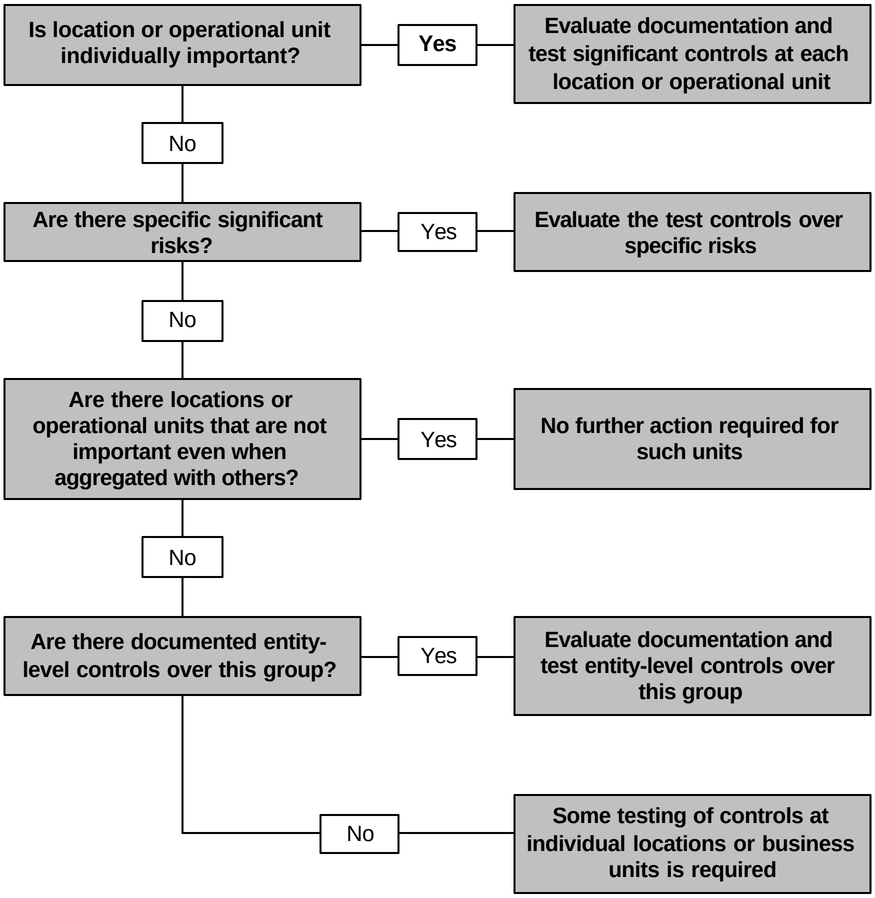
Step 5a: Identify locations subject to testing and assess coverage.

To determine which locations must be included in the assessment of internal control over financial reporting, the assessment team should evaluate each location's relative financial significance and the risk of material misstatement associated with that location. To evaluate the significance of each location, the assessment team should prepare financial information by location. The information should be reconciled with reported balances to ensure completeness.

For locations that are individually important (defined in Step 6A below), the assessment team should document and test controls for all significant accounts and disclosures. Generally, a relatively small number of locations will encompass a large portion of the Department/Component's operations and net position, making them financially significant. However, the assessment team cannot test a large portion of the entity's operations and net position by selecting a relatively small number of locations. The assessment team must select additional locations or consider whether a sampling technique may be appropriate. Testing entity-level controls is not a substitute for testing controls for a large portion of the entity's operations or net position.

The following decision tree illustrates the steps that should be taken in this categorization process:

Figure 9: Multi-Location Categorization Process[19]


Is location or operational unit individually important?
Yes
Evaluate documentation and test significant controls at each location or operational unit
No
Are there specific significant risks?
Yes
Evaluate the test controls over specific risks
No
Are there locations or operational units that are not important even when aggregated with others?
Yes
No further action required for such units
No
Are there documented entity-level controls over this group?
Yes
Evaluate documentation and test entity-level controls over this group
No
Some testing of controls at individual locations or business units is required

Step 5.a.1. Determine which locations/operating units are individually important.

The goal of this step is to determine which locations are individually important (financially significant) and thus yield sufficient coverage using meaningful quantitative metrics (reflective of the organization's specific risks). Although specific percentages to determine coverage have not been defined for the Federal Government, common practice for SOX involves obtaining at least 60 to 70 percent coverage of the entity's operations and net position (including individually important locations and the specific risk areas discussed in Step 6B). Ideally, these locations will represent a relatively small number of the entity's total locations. Individually important locations are generally those meeting at least one of the balance sheet or statement of net cost consolidated metrics that are shown below[20]. The suggested maximum consolidated metrics to be used for selecting individually important locations/operating units are:

- > 5 percent of annual appropriations
- > 5 percent of gross cost

[19] Adapted from chart provided in PCAOB AS2.

[20] These are best practice metrics suggested for companies under the requirements of AS2

- > 5 percent of total assets
- > 5 percent of net position (if applicable)

These metrics may need to be adjusted to take into account different organizational structures. For example, if the organization operates in a decentralized manner with multiple, similarly sized operating units, the percentages that it uses to determine individually important locations may need to be reduced to 1 or 2 percent of the indicated metrics to obtain sufficient coverage.

The quantitative measure should be tailored to the Department/Component. The quantitative metrics should be derived from the organization's consolidated financial statements. At a minimum, the assessment team must use one balance sheet metric (e.g., total assets or net position) and one statement of net cost metric (e.g., revenue or gross cost) in connection with the quantitative assessment.

For Example: *(in millions)*

Balance Sheet Metric (FY 2004 unaudited) –

```
Total Assets   =  $50,806
                     X .05
                    $2,540
```

Statement of Net Cost Metric (FY 2004 unaudited) –

```
Total Net Cost   =  $33,128
                       X .05
                      $1,656
```

When identifying individually important locations, the most recent fiscal year-end (e.g., the consolidated statements dated September 30, 200X) should be used. If the financial results that management has chosen as the source information have been substantially impacted by unusual events or significant transactions, the assessment team should modify the results so that they do not reflect those events and transactions. Any budget or prior year data also should be updated to reflect any significant anticipated changes.

After identifying individually important locations based upon the selected metrics, management should assess coverage. As indicated, coverage over at least 60 to 70 percent of the consolidated metric should be obtained (including those specific risk areas discussed in Step 6B). The assessment team must document the rationale for the appropriateness of the selected financial metrics.

The design and operating effectiveness of internal control over financial reporting must be tested at all individually important locations even if the Department/Component can obtain a large portion of coverage without including an individually important location[21]. For example, assume that the Department has locations that represent the following percentages of net costs and total assets:

Location A	30%
Location B	20%
Location C	15%
Location D	10%

[21] PCAOB AS2.

Location E	10%
Location F – M	Each less than 5%

Based on these facts, testing of the design and operating effectiveness of internal control over financial reporting for all significant accounts and disclosures should be performed at locations A, B, C, D, and E despite the Department's ability to obtain 65 percent coverage from locations A, B, and C. This is because locations D and E are individually important.

Point of Focus 6

Planning Consideration: Testing at individually important locations

The assessment team should plan to test controls over all relevant assertions for each significant account balance or disclosure at an individually important location for which the selected accounts are material at the location. Additionally, management would test entity-level controls from two perspectives:

1. *The perspective of the location - what are the control environment, risk assessment, information and communication, and monitoring functions specific to the location?*
2. *The perspective of looking "upward" regarding controls directed by corporate headquarters - the assessment team should ensure that entity-level controls are working according to their design (e.g., the corporate accounting policy manual is being used at the location).*

A significant account (at the consolidated financial statement level) at an individually important location need not be tested if it is immaterial at that location. However, if an account is material at a location that is not individually important, the controls over all relevant assertions for that account should be tested. See Step 6B for discussion of the identification of specific risks.

Coverage at the Individual Account level

Typically, coverage of 60 to 70 percent of the selected consolidated metrics (i.e., total revenues, total assets, total net position, or total gross cost) will translate into coverage of approximately 60 to 70 percent at the level of a significant account or disclosure. In some situations, coverage of a significant account or disclosure will fall below 60 percent. A large portion of coverage is determined at the overall financial statement level not an individual account level. As a result, the entity is not required to add more locations to attain a minimum coverage level of 60 percent for all significant accounts and disclosures. However, it will be important for the assessment team to exercise judgment in these situations.

If the coverage of a significant line item's account or disclosure is below 50 percent, the assessment team should reassess its identification of specific significant risks and consider selecting additional locations to gain sufficient evidence of the operating effectiveness of the controls related to that account or disclosure. Substantially low coverage (below 50%) may indicate that a specific significant risk has been overlooked in the initial planning process.

Step 5.a.2. With respect to the remaining locations, determine whether there are specific significant risks in specific areas.

Even though a location's relative financial significance to the Department/Component's consolidated financial position or operations may be small, the location may still be responsible for certain areas that expose the organization to the risk of a material misstatement. For locations carrying specific risks (e.g., a location responsible for Treasury reporting) that could result in a material misstatement, the assessment team should document and test controls that mitigate those specific risks, as well as document its rationale for categorizing certain factors as specific risks.

Examples of factors that may indicate increased risk in an area at a location include:

- The assessment team risk assessment
- Internal or external audit findings and recommendations
- Significant, unusual, or non-recurring transactions
- Significant individual account balances
- Changes in management

Specific risk locations contribute to the consolidated coverage of the selected quantitative metrics when the accounts affected by the specific significant risk are directly included in the selected metrics. For example, if the specific risk and the selected statement of net cost metric are both revenue, the revenue from the specific risk location would be included in the coverage calculation. However, if the statement of net cost metric is gross cost and the specific risk is revenue, the gross cost from the specific risk location would not be included in the calculation of coverage of the gross cost.

Achieving the Right Coverage

If the individually important and specific risk locations do not provide management with the appropriate coverage, the assessment team should:

- re-evaluate the specific risks and ensure all have been identified; and
- re-evaluate and lower the quantitative metrics used to identify the individually important locations to select additional locations to obtain the necessary coverage.

If lowering the selected metrics results in additional locations that bring total coverage to an amount more than is necessary, all locations that meet this lower threshold still should be included (i.e., management cannot select only some of the individually important locations that represent more than the selected metric to arrive at coverage of 60 to 70 percent).

Step 5.a.3. If the remaining *aggregated* locations are insignificant and thus could not result in a material misstatement to the financial statements, no further procedures are necessary.

With respect to locations that cannot cause, either individually or in the aggregate, a material misstatement in the organization's financial statements, the assessment team need not perform procedures at those locations. The aggregate of these individually unimportant locations would typically be less than five percent of the quantitative thresholds for the individually important locations and that none would have specific qualitative risks.

Step 5.a.4. If the remaining locations are significant when aggregated, management will need to consider the following:

1. If entity-level controls are effectively designed and operating, the assessment team should obtain assurance through documentation and testing of entity-level controls. In addition, the assessment

team may determine that other evidence is necessary. (Entity-Level controls are discussed later in this section.)

2. If entity-level controls are *not* effectively designed or operating, the assessment team must perform testing of control activities at these locations to obtain the necessary assurance that such controls are designed and operating effectively.

If entity-level controls are in place, the assessment team will be required to document and test them. To conclude that entity-level controls are operating effectively at these locations, the assessment team ordinarily would need to visit at least some of the locations and assess that the controls are operating effectively. In addition, the assessment team may determine that evidence such as walkthroughs, self-assessments, reviews performed by a quality assurance or internal control operating unit, or monitoring controls is necessary to conclude that control activities at these locations are designed and operating effectively.

If (1) the Department/Component does not have entity-level controls in place at these locations or (2) the controls are not reliable, the assessment team will need to determine the nature, timing, and extent of the procedures to be performed at each location to obtain the necessary assurance.

In evaluating which locations should undergo entity-level control testing and the controls to be tested, the following factors should be considered[22]:

- The relative financial significance of each location;
- The risk of material misstatement arising from each location;
- The similarity of operations and internal control over financial reporting at the various locations;
- The degree to which processes and financial reporting applications are centralized;
- The effectiveness of the control environment, particularly management's direct control over the exercise of authority delegated to others and its ability to supervise activities effectively at the various locations;
- The nature and amount of transactions executed and the related assets at the various locations;
- The degree to which a location could create an obligation on the part of the organization; and
- The assessment team's risk assessment process and analysis for excluding a location from its assessment of internal control over financial reporting.

Step 5b: Map locations to the processes/cycles and sub-processes/sub-cycles identified previously.

The next step is to map significant line items to sub-processes/sub-cycles at each location. For example:

- A location may be responsible only for the controls covering the payroll sub-processes/sub-cycles.
- Another location may be responsible only for the controls covering the accounts payable sub-processes/sub-cycles.

[22] PCAOB AS2.

- A location may be responsible for controls covering Treasury reporting and budgeting sub-processes/sub-cycles.

Appendices G and H Include examples of how mappings of significant line items and related accounts and disclosures to cycles/processes, and sub-cycles/sub-processes may be performed and documented.

Figure 10: Recap for Determining Multiple-Location Coverage

Minimum Account Balance Coverage	Location	Planned Procedures
60 – 70%	Individually important locations and line items with specific risks	The ICC (at the consolidated level) and the assessment teams (at the Component level) will determine individually important locations and line items with specific risks. The assessment team will be required to perform detailed evaluation and tests of controls over significant (or “specific risk”) accounts and disclosures at that location and testing of entity-level controls.
25 – 35%	Locations considered important when aggregated	The ICC (at the consolidated level) and the assessment teams (at the Component level) will determine locations considered important when aggregated. The ICC (at the Department-wide level) and the assessment teams (at the Component level) will be required to evaluate and test entity-level controls, if applicable, and consider obtaining other evidence or perform some tests of controls at locations if entity-level controls do not exist.
<5%	Immaterial locations, individually and in the aggregate	The ICC (at the consolidated level) and the assessment teams (at the Component level) will determine immaterial locations, individually and in aggregate. No testing required by the assessment team.

3.6 – Step 6 – Other Considerations

The period-end reporting process, application and general computer controls, entity-level controls, laws and compliance, mergers, and new system integrations are not separate Components of internal control; however, they are important elements of an entity's internal control over financial reporting, and thus are discussed separately below.

3.6.1 – Step 6a – Period-End Reporting Process

The period-end financial reporting process is always a significant process because of its importance to financial reporting and the financial statements. Evaluating the design and effectiveness of controls for the period-end financial reporting process is an important step in the overall assessment of internal control over financial reporting.

Figure 11: Period-End Reporting Process

The period-end financial reporting process includes…	The Assessment Team should plan to evaluate…
The procedures used to enter transaction totals into the general ledger. The procedures used to initiate, authorize, record, and process journal entries in the general ledger. Other procedures used to record recurring and nonrecurring adjustments to the annual and quarterly financial statements, such as consolidating adjustments, report combinations, and classifications. Procedures for drafting annual and quarterly financial statements and related disclosures.	The automated and manual inputs, procedures performed, and outputs of the processes the organization uses to produce its annual and quarterly financial statements. The extent of information technology involvement in each period-end financial reporting process element. Who participates from management. The number of locations involved. The types of adjusting entries. The nature and extent of the oversight of the process by appropriate parties, including management and the Office of Inspector General. The controls over the consolidation process. The method for establishing and monitoring the selection and consistent application of accounting policies. The use of manual spreadsheets and manually compiled data in the consolidation process.

The Department/Component's management is responsible for the controls over the period-end reporting process. The external auditors should not participate in the execution of these controls or be considered a part of management's control over the period-end reporting process. Management must have the expertise (1) to select and apply accounting policies and (2) to form a view over accounting and reporting matters. Management should be able to demonstrate how it develops, approves, communicates, implements, and monitors accounting policies. These policies and procedures should be documented and tested as part of the assessment process.

The period-end reporting process often involves multiple levels of the entity. Thus, it is likely that evaluating and testing the period-end reporting process will extend beyond the Departmental level. For example, the following items (if applicable) should be included in the evaluation of the period-end reporting process:

- Manual journal entries that are posted during the process of consolidating the Components at the Departmental level (e.g., consolidation entries, elimination entries, or other "top level" adjustments);
- Manual journal entries that are posted during Component consolidation that is then submitted to the Department for inclusion in the Department-wide consolidation;
- Manual journal entries posted directly to the general ledger before consolidation at the Component or Department-wide level (i.e., as part of the reconciliation of a sub-ledger with the general ledger); and

- Systematic and transactional postings to the general ledger throughout the course of operations (i.e., posting of sub-ledger account balances to the general ledger).

Selecting and applying accounting policies that are consistently communicated and implemented across the Department/Component's locations and operating units is an important control activity in the period-end reporting process. Management should consider the following control activities in its period-end reporting process as it relates to the selection and application of appropriate accounting policies:

- Monitor activities of the standard-setting bodies through
  - newsletters, databases, and websites
  - participation in industry and professional committees and conferences
- Develop procedures to communicate new accounting policies throughout the organization
- Ensure policies are established for higher risk (i.e., significant, complex, judgmental) accounts or transactions
- Develop and document accounting policies
- Employ appropriately skilled individuals
- Provide training for individuals responsible for applying policies
- Require CFO approval of critical accounting policies

Disclosures

Disclosures are an important Component of financial reporting which should be considered during the planning phase of the assessment and tested and evaluated during the appropriate phases of the assessment. The assessment team should ask the following:

- Who is responsible for compiling/computing each of the disclosures in the annual reports?
- What process is in place to ensure that disclosures meet the requirements of FASAB, GAAP, and other regulatory bodies/standards?
- What are the sources of information that support the disclosure process?
- How do the individuals who are responsible for the disclosures ensure that the source information is accurate, valid, and complete?
- Who reviews the disclosures upon completion?
- What are the inputs, procedures, and outputs that are used to produce the financial statements and disclosures?
- How have the organization's financial management office reviewed the control over the financial reporting and disclosure process to ensure all information is properly disclosed?
- How does management ensure that subsequent events are identified for disclosure?
- How is the segregation of duties addressed within the period-end reporting process?
- If spreadsheets are used to summarize financial data for disclosure purposes, what controls cover the input and formulas in the spreadsheet?

Timing Considerations

Although many of the period-end reporting controls are applied after year-end (i.e., as the year-end financial statements are being prepared), those controls are relevant to the organization's internal control over financial reporting at the reporting date and thus must be considered.

The assessment team should plan to review the year-end processes and procedures before year-end to ensure that they are designed effectively. If deficiencies are detected during year-end testing of these "annual" controls, the assessment team will not be able to remediate until the following year.

Additionally, the assessment team should plan the timing of testing of quarterly financial reporting processes to ensure that sufficient time is allowed for any necessary remediation efforts.

3.6.2 – Step 6b – Accounting Estimates and Judgments

Control over accounting estimates and judgments are an important part of internal control over financial reporting. Weak controls in this area could negate an otherwise strong system of internal control. Accounting estimates and judgments often pertain to areas, such as:

- Legal accruals, including benefit payment accruals
- Environmental accruals
- Impairment analysis and charges

The assessment team should understand and plan to assess the following for estimates and judgments;

- Which accounts, estimates, and judgments are manually adjusted at the end of a period;
- Who prepares the journal entries, estimates, and judgments;
- Who reviews the journal entries, as well as the assumptions surrounding the estimates and judgments;
- What supporting documentation is maintained on file to support the entries; and
- Whether the procedures during the year are different than at year-end.

3.6.3 – Step 6c – Control Activities Specific for Information Systems

An important aspect of internal control is information system controls. Information system controls are comprised of both general computer and application controls. General computer controls apply to all information system networks, operating systems, and databases supporting business applications and data. Application controls cover the processing of data within application software. The degree to which an entity can rely on the integrity of information processing and the effectiveness of automated controls, including automated accounting procedures (i.e., calculations and automated postings to accounts) (application controls), depends on the effectiveness of general computer controls. OMB Circular A-123 states, "general and application controls over information systems are interrelated; both are needed to ensure complete and accurate information processing."

There are a myriad of federal laws, directives and criteria pertaining to information technology internal controls that DHS and its Components must address. During the assessment process, the assessment team should consider requirements dictated by these other laws and regulations in order to gain efficiencies. The assessment team may be able to avoid a duplication of efforts by maintaining a consolidated, detailed checklist that itemizes and cross-references the various requirements and associated reporting dates, if applicable. By doing so, the Department and the assessment team may be able to streamline its approach to these compliance areas, which often overlap.

Listed below are some of the laws, directives and criteria that agencies must adhere to with regards to information technology controls. These references are not intended to be all-inclusive:

Clinger-Cohen Act of 1996. This Act linked computer security to agency capital planning and budgeting processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.

Computer Security Act of 1987. The Computer Security Act requires that federal agencies provide mandatory periodic training in computer security awareness and accepted security practice to all employees involved with the management, use, or operation of a federal computer system within or under the supervision of a federal agency.

Federal Information Security Management Act (FISMA). This Act requires an annual independent evaluation of the information security program and practices of each agency. The Inspector General or the independent evaluator performing the evaluation will use an audit, relating to programs or practices of the applicable agency in accordance with government auditing standards.

The Federal Managers' Financial Integrity Act (FMFIA). This Act requires Federal managers to establish a continuous process for valuating, improving, and reporting on the internal control and accounting systems for which they are responsible. The FMFIA requires that each year, the head of each executive agency subject to the Act shall submit a report to the President and Congress on the status of internal controls and financial systems that protect the integrity of agency programs and administrative activities.

Office of Management and Budget Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources." OMB Circular A-130 establishes a minimum set of controls to be included in federal information technology (IT) security programs. Specifically, the circular requires that a management official authorize, in writing, the use of each IT system based on implementation of its system security plan before beginning or significantly changing processing. Also, OMB Circular A-130 requires that all individuals be appropriately trained in how to fulfill their security responsibilities before they are granted access to a system or application.

Presidential Decision Directive 63, "Protecting America's Critical Infrastructures." This directive specifies agency responsibilities for protecting the nation's infrastructure; assessing vulnerabilities of public and private sectors; and eliminating vulnerabilities.

Presidential Decision Directive 67, "Ensuring Constitutional Government and Continuity of Government." Relates to ensuring constitutional government, continuity of operations planning (COOP), and continuity of government (COG) operations.

Government Accountability Office "Federal Information System Control Audit Manual" (FISCAM). The methodology used in this manual provides guidance to auditors in evaluating general controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.

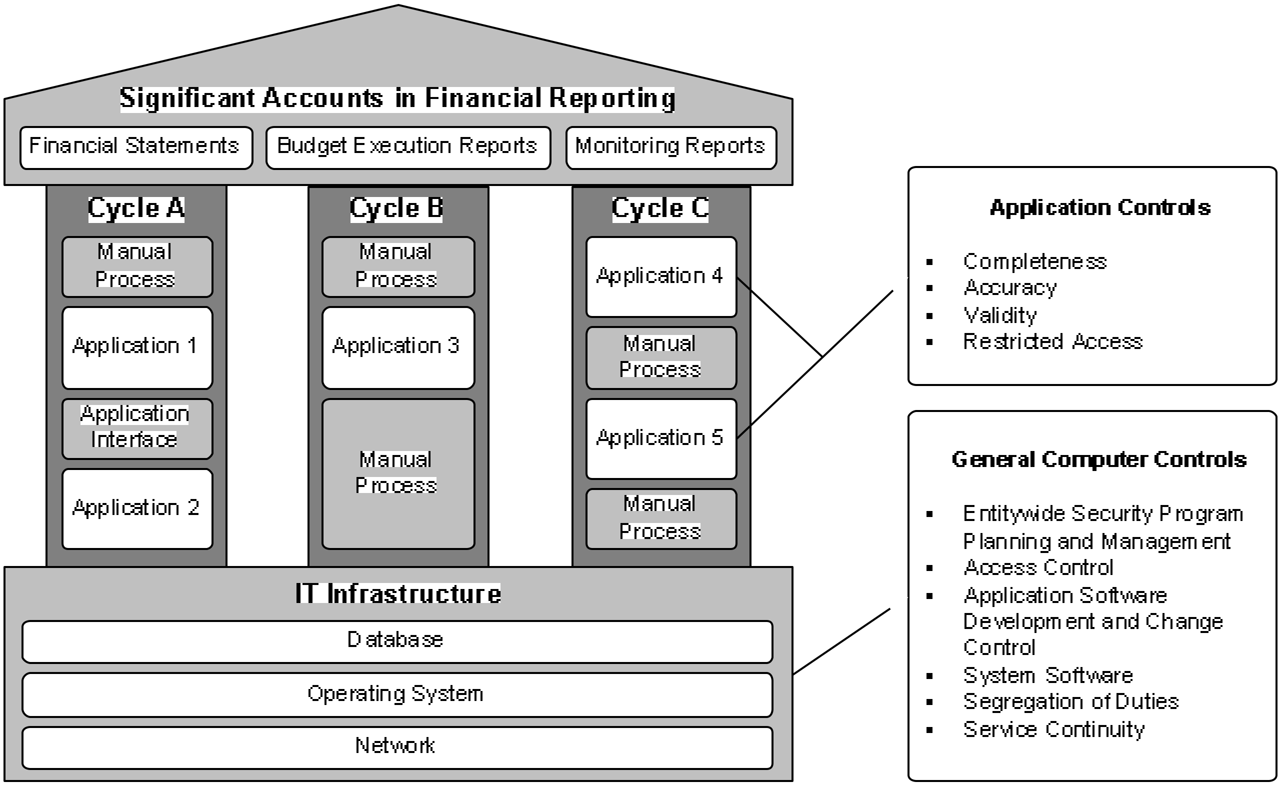
Department's "Information Technology Security Standards." These standards establish uniform procedures for the implementation and protection of Department IT systems that store, process, or transmit classified and unclassified information.

OMB Memorandum M00-07, "Incorporating and Funding Security in Information Systems Investments," provides guidance to agencies on accomplishing the requirement to practice security planning throughout the life cycle of each system.

During the controls self-assessment, DHS management should also consider compliance with other special publications, i.e. National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS), as well as DHS-specific guidance or policies related to information technology.

The following diagram illustrates the relationship between the information technology (IT) infrastructure, over which general computer controls are placed, and applications, over which application controls are placed. Notice that applications are part of the overall business cycle. This diagram shows that the lack of sufficient general computer and application controls negatively impacts the organization's internal control over financial reporting.

Figure 12: Impact of the Lack of Sufficient General Computer and Application Controls



Application Controls

Significant processes/cycles that involve computer programs (applications) will generally require some degree of additional controls. These controls, referred to as application controls, include the automated controls built into the application (such as computerized edit checks and required passwords) and the manual controls surrounding the application (such as manual interface reconciliations, management sign-offs, and audit log reviews). Sufficient automated and manual control activities should be in place to address the information processing objectives/CAVR (completeness, accuracy, validity, and restricted access) for each transaction processed by the application.

The in-scope applications are those that play a role within the processes/cycles that are considered significant to the financial statements. The assessment team must understand how financial information is generated and map the financial statements and processes/cycles to the applications that enable the initiation, authorization, recording, and processing of the information.

General Computer Controls

Unlike application controls, which are a part of the overall process controls, general computer controls are pervasive and over-arching. In other words, general controls affect every cycle that uses computer applications to perform a specific function within that cycle. This is because general computer controls are used to manage and control the organization's information technology infrastructure (i.e. Network, Operating Systems, and Databases). Underlying the locations and the processes/cycles are the computer systems, applications, and data centers that facilitate information processing throughout the organization. The processing of information by systems is a key aspect of the information and communication Component of internal control. In most entities, the integrity of the financial statements greatly depends on the completeness, accuracy, and timeliness of the information flowing through its systems. Also, automated controls over the financial statement assertions are reliant upon the proper functioning of the underlying applications and their supporting information technology infrastructure.

The general computer control scoping decisions will vary based upon how the organization's information technology is organized and managed. Once management has determined significant processes/cycles and their associated significant applications, they can identify the supporting information technology infrastructure (data centers and information technology environments). Only those general computer controls that support processes and applications that, in turn, support significant financial statements accounts and disclosures, need to be documented and tested.

Information processing and related controls must also be considered at the technology infrastructure level, including the database, operating system, internal network, and perimeter network levels. For each of these infrastructure layers, management must consider the control activities prescribed by Chapter Three of the Federal Information System Controls Audit Manual (FISCAM): "Evaluating and Testing General Controls." This chapter describes six major categories of general controls that should be considered, as follows:

- Entity-wide security program planning and management that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an entity's computer-related controls;
- Access controls that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;
- Application software development and change controls that prevent unauthorized programs or modifications to an existing program from being implemented;
- System software controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system;
- Segregation of duties that consists of policies, procedures, and an organizational structure established so one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records; and
- Service continuity controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Each of these FISCAM categories, often referred to as Domains, is further discussed in Section Four - Documentation and in Appendix D - Index of Definitions and Key Terms at the end of this document. Each organization should use judgment in tailoring its approach to evaluating controls related to each of these domains, so it is appropriate for the size and complexity of the organization's unique IT environment.

Mapping

Similar to the requirements for mapping Significant Line items to Processes/Cycles and locations, as discussed in Appendix G, the assessment team should map applications to the in-scope processes/cycles. Without appropriate mapping, the assessment team may inadvertently exclude certain applications or parts of the IT infrastructure that are not managed by the data center(s). The assessment team must be able to demonstrate that necessary coverage over the IT function has been addressed through its procedures.

Point of Focus 7

Information Technology Security Accountability

Information technology security, which comprises the controls governing access to an organization's computer systems, is vital to safeguarding organizational assets, as well as to maintaining the integrity of financial reporting. IT security controls ensure that only the appropriate people can access and change key financial data. Without adequate security, the integrity of the financial data may be compromised or impaired. Information security consists of (1) perimeter security, which protects an organization's network and computers and (2) application-level security, which limits access to transactions and other data within a computer application, as well as enforces segregation of duties. The assessment of perimeter security should be the responsibility of the IT organization. Because application-level security is tied to the organization's process controls, responsibility for documenting and assessing application-level security should rest with the individuals (or teams) responsible for the related process.

Management should also consider security access to spreadsheets and other financial data residing on shared servers.

3.6.4 – Step 6d – Compliance with Laws and Regulations

The assessment team must consider the impact of laws and regulations that have a direct and material impact on financial reporting. OMB Circular A-123 requires Agencies to develop and implement controls to ensure that transactions are processed in accordance with applicable laws and regulations. Therefore, the assessment team should complete its assessment of internal controls against the transactions, which when aggregated would have a direct and material affect on the financial statements (direct and material effect is defined below). The assessment team should work closely with the Chief Financial Officer and the Office of General Counsel to determine the provisions of laws and regulations that apply to the entity's financial reporting. Once a complete list of laws and regulations has been assembled, the assessment team should identify the controls that ensure compliance and ensure these controls are included in the planning of the project and ultimately management's assessment.

A direct effect means that the provision specifies[23]:

- The nature and/or dollar amount of transactions that may be incurred (such as obligation, outlay, or borrowing restrictions),

[23] Definition of direct effect and examples obtained from the GAO/PCIE Financial Audit Manual. The concept of direct effect is discussed in AU Section 801 (Statement of Auditing Standards (SAS) No. 74) and AU 317 (SAS No. 54).

- The method used to record such transactions (such as revenue recognition policies), or
- The nature and extent of information to be reported or disclosed in the annual financial statements (such as the statement of budgetary resources).

For example, entity-enabling legislation may contain provisions that limit the nature and amount of obligations or outlays and therefore have a direct effect on determining amounts in the financial statements. If a provision's effect on the financial statements is limited to contingent liabilities as a result of noncompliance (typically for fines, penalties, and interest), such a provision does not have a direct effect on determining financial statement amounts. Laws identified by the auditor that have a direct effect might include (1) new laws and regulations (not yet reflected on OMB's list) and (2) entity-specific laws and regulations.

In contrast, indirect laws relate more to the entity's operating aspects than to its financial and accounting aspects, and their financial statement effect is indirect. In other words, their effect may be limited to recording or disclosing liabilities arising from noncompliance. Examples of indirect laws and regulations include those related to environmental protection and occupational safety and health.

In addition to having a direct effect, laws and regulations considered in this section should have a material effect on the financial statements. Refer to Section 3.4 (Point of Focus # 3) for definition of Materiality. Examples of applicable laws may include, but not be limited to the following:

- The Agency's enabling legislation,
- Antideficiency Act
- Provisions Governing Claims of the United States Government (31 U.S.C. 3711-3720E), including provisions of the Debt Collection Improvement Act of 1996,
- Federal Credit Reform Act of 1990,
- Pay and Allowance System for Civilian Employees (5 U.S.C. 5332 and 5343, 29 U.S.C. 206),
- Civil Service Retirement Act
- Prompt Payment Act,
- The Improper Payments Information Act of 2002
- Federal Managers' Financial Integrity Act of 1982(FMFIA)
- Federal Information Security Management Act
- Improper Payments Information Act of 2002 (IPIA)

3.6.5 – Step 6e – Mergers/Consolidations

Currently, there is no Federal guidance that dictates how mergers or consolidations impact the assessment of internal control. For the time being, the PCAOB has issued some general guidelines that provide a framework for the Department to follow until more authoritative guidance is issued. Pending further guidance general guidelines or rules to consider when a merger or consolidation occurs include:

1. If it is not possible to include a merged entity into the assessment, the assessment team may exclude the entity for up to one year.

2. If the entity is excluded, the assertions of internal control over financial reporting must disclose the entity excluded from the assessment.

Another area for consideration is the transition from the old entity to the new one. Regardless of whether the one-year option is taken, the assessment team will have to address integration of the new entity into the overall internal control framework at some point. The transition of internal control will likely take on a combination of the following forms:

1. Change each control and process to make it compatible with the new entity's internal control and thus reduce efforts to comply with the requirements of OMB Circular A-123.

2. Leave controls under the old entity's current control structure and perform the assessment, thus reducing work required to alter existing control structures.

3. In the case where a smaller portion of an organization is carved out and merged into a different organization, the two agencies may consider a service agreement between the two entities. Certain functions would continue to be performed at the old entity on behalf of the merged portion. The old entity would be required to assess those shared services and issue a Type II SAS 70 report (see 3.9 Use of Service Organization). The new entity would rely on the Type II SAS 70 report for management's assertions.

Each option has pros and cons. Option one requires a large investment in changing controls to the new entity's standard. Option two requires additional controls work to be done during the assessment. Option three develops ties and dependencies that may last for some time.

3.6.6 – Step 6f – New Systems (e.g., eMerge[2])

New systems generally need to be included in the assessment if they impact the financial reporting in the current fiscal year. Conversely, if the system is in development, but will not go live in the current fiscal year, generally it will not need to be included in the project.

The application controls for the new systems should be documented and assessed using the same process as all other in-scope systems. Please see specific sections addressing application controls within this guide for detailed instructions on documenting and assessing application controls.

FISCAM Section CC-1.1: *A System Development Life Cycle (SDLC) Methodology has been implemented;* specifically addresses the general computer controls that should have been addressed during system implementation. FISCAM specifies that:

> The entity should have a documented SDLC methodology that details the procedures that are to be followed when applications are being designed and developed, as well as when they are subsequently modified. The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations; assessing the costs and benefits of various options, including the feasibility of using off-the-shelf software; and designing, developing, testing, and approving new systems and system modifications. Especially for new systems being developed or for major enhancements to existing systems, it is important that SDLC require approving design features at key points during the design and development process.

See specific sections addressing general computer controls within this guide for detailed instructions on documenting and assessing general computer controls.

Additionally, the assessment team should determine if there were any major disruptions to the internal control structure during system implementation. The team should document and assess controls at the time of and as part of implementations. The Component assessment team should also note any problems that were encountered during new system implementation and the effect that these problems had on the 'go live' date. Implementations that occur late in the fiscal year pose a higher-threat to management's assertion and should be planned and executed carefully.

3.7 – Step 7: Use of Service Organizations

Some organizations may use outside service organizations to process financial data. Service organizations include cross-servicing Components, federal agencies, states organizations, and commercial companies. Management is ultimately responsible for the internal control over their financial information and, therefore, the assessment team may need to assess the design and operating effectiveness of the service organization's internal control, including all five Components of internal control. This responsibility is consistent with management's obligations under OMB Circular A-123 stating, "management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations."

The assessment team should create a summary of its service organizations, detailing key information about the organization's outsourcing arrangement with each service organization (i.e., summarizing the services provided, indicating whether the organization is allowed to audit the service organization, determining whether a SAS 70 report exists, and noting the expiration date of the contract) and track the results of and rationale for decisions, based on the decision tree below. To develop an accurate summary, an entity should start with the list of vendor contracts that are typically maintained by the Department/Component's procurement Department. It is likely that the assessment team will identify additional service organizations in the planning and documentation phases of this project. The assessment team will then need to determine which procedures to apply to each outsourcing arrangement.

The assessment team should consider the following steps when evaluating the procedures to perform over its service organizations:

1. Determine if a service organization is being used.

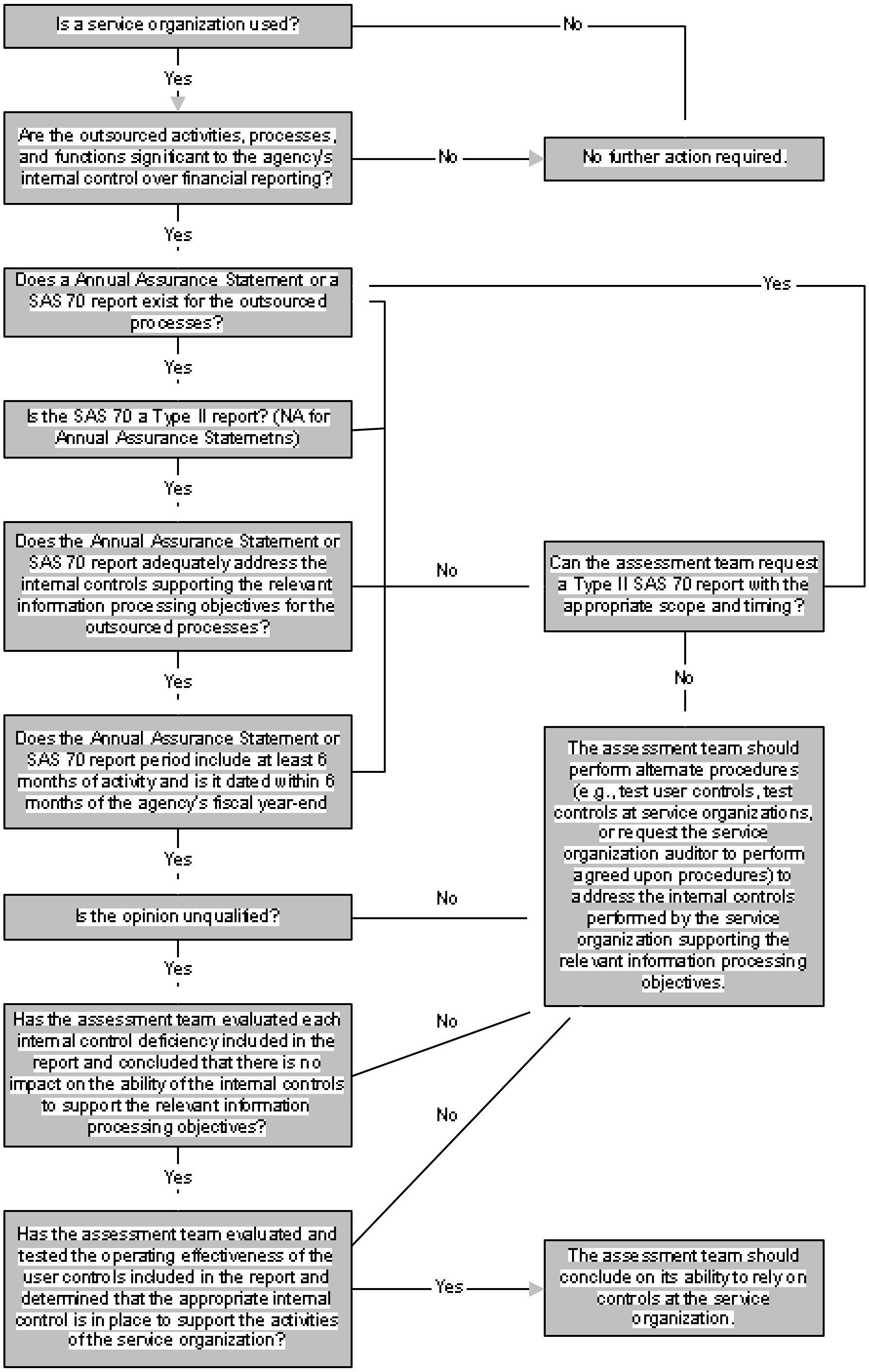
2. Determine if the outsourced activities, processes, and functions are significant to the entity's internal control over financial reporting.

3. Determine if an annual assurance statement (cross-servicing organization) or a SAS 70 (commercial company) exists and is sufficient in scope.

4. If an annual assurance statement or SAS 70 does not exist, determine alternative procedures.

This process is summarized in the decision tree below and explained further in the remainder of this section.

Figure 13: Annual Assurance Statement or SAS 70 Decision Tree


Is a service organization used?
No
Yes
Are the outsourced activities, processes, and functions significant to the agency's internal control over financial reporting?
No
No further action required.
Yes
Does a Annual Assurance Statement or a SAS 70 report exist for the outsourced processes?
Yes
Yes
Is the SAS 70 a Type II report? (NA for Annual Assurance Statemetns)
Yes
Does the Annual Assurance Statement or SAS 70 report adequately address the internal controls supporting the relevant information processing objectives for the outsourced processes?
No
Can the assessment team request a Type II SAS 70 report with the appropriate scope and timing?
Yes
No
Does the Annual Assurance Statement or SAS 70 report period include at least 6 months of activity and is it dated within 6 months of the agency's fiscal year-end
The assessment team should perform alternate procedures (e.g., test user controls, test controls at service organizations, or request the service organization auditor to perform agreed upon procedures) to address the internal controls performed by the service organization supporting the relevant information processing objectives.
Yes
Is the opinion unqualified?
No
Yes
Has the assessment team evaluated each internal control deficiency included in the report and concluded that there is no impact on the ability of the internal controls to support the relevant information processing objectives?
No
No
Yes
Has the assessment team evaluated and tested the operating effectiveness of the user controls included in the report and determined that the appropriate internal control is in place to support the activities of the service organization?
Yes
The assessment team should conclude on its ability to rely on controls at the service organization.

3.7.1 – Step 7a – Determine if a Service Organization Is Being Used

Many agencies outsource activities to service organizations (other agencies or commercial companies). However, not all outsourced situations will be within the scope of this assessment. Generally, an outsourcing situation would need to be considered for management's assessment only when the outsourced activities constitute a significant process or function performed by a third party that generates information significant to the financial reporting process.

When identifying service organizations, the assessment team should distinguish between service organizations and specialists. For example, management may use a specialist to perform:

- Valuations;
- Determinations of physical characteristics relating to quantity on hand or condition;
- Determinations of amounts derived by using specialized techniques or methods; and
- Interpretations of technical requirements, regulations, or agreements.

These specialists are not part of an outsourced process and would not need to be evaluated as if they were part of the entity's internal control over financial reporting. However, the output of a specialist's work is often significant to the financial statements. Thus, management should have controls in place (such as a means to evaluate the specialist's professional qualifications) to assess whether the specialist has the required skills and knowledge in the particular field to make an appropriate determination. Component management and the assessment team should also understand[24]:

- The objectives and scope of the specialist's work;
- The methods or assumptions used; and
- How the methods or assumptions used compare to those used in the preceding period.

3.7.2 – Step 7b – Determine if the Outsourced Activities, Processes, and Functions are Significant to the Entity's Internal Control over Financial Reporting

The assessment team needs to consider only outsourced operations that are part of processes the assessment team deems significant to its internal control over financial reporting. Auditing Standard Section No. 324, *Service Organizations* (SAS 70 or AU 324), indicates that activities are considered part of an organization's internal control if they affect any of the following:

- The classes of transactions that are significant to the entity's financial statements;
- The procedures, both automated and manual, by which the organization's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements;
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial statements involved in initiating, recording, processing, and reporting the organization's transactions;

[24] Auditing Standard Section No. 336, *Using the Work of a Specialist.*

- How the entity's information system captures other events and conditions that are significant to the financial statements; and
- The financial reporting process used to prepare the organization's financial statements, including significant accounting estimates and disclosures.

When addressing whether a particular service organization affects the Component's internal control over financial reporting, the assessment team must consider the significance of the financial statement assertions and the information processing objectives/CAVR for the process being outsourced. If the controls covering one or more information processing objectives/CAVR or financial statement assertions reside principally at the service organization, it is likely that the service organization affects the financial reporting process and will need to be evaluated.

If the activities being performed at the service organization are considered part of the organization's internal control over financial reporting, the assessment team must determine the extent of procedures, which may include:

- Obtaining an annual assurance statement (cross-servicing Component) or a Type II SAS 70 service auditor's report (federal agency, state organization or commercial company) and evaluating the user organization's controls over the activities of the service organization (including those user controls listed in these reports);
- Performing tests of controls at the service organization;
- Obtaining a report on the application of agreed upon procedures that describes the tests of relevant controls; and
- Performing tests of the user organization's controls.

Depending on the significance and risk of the outsourced process, a combination of these options may be required.

3.7.3 – Step 7c – Determine if an annual assurance statement (cross-servicing Component) or a SAS 70 (commercial company) exists and is sufficient in scope.

Annual Assurance Statements

If a Component uses the services of another Component (cross-servicing Component) the serviced Component must obtain the serviced Component annual assurance statement. The annual assurance statement must include an assessment of the effectiveness of the Component's internal control over financial reporting as it relates to the services being provided.

SAS 70s

A SAS 70 must be obtained if the service is being provided by an organization outside of DHS (i.e. Other Federal Agencies, State Agencies, and Commercial Organizations). SAS 70 allows a service organization (such as one performing internal accounting services) to obtain a single audit report for use by its clients' auditors to plan and conduct audits of financial statements. One of the objectives of SAS 70 was to preclude the need for each user auditor to conduct its own audit of the service organization's controls.

If the assessment team determines that the controls at the service organization must be assessed, the assessment team should determine if a Type II SAS 70 report exists. If so, the assessment team should evaluate whether or not the report adequately addresses the information processing objectives/CAVR relevant to the organization's needs. If a Type II SAS 70 report does not exist or the report is not adequate to meet the assessment team's needs, an adequate report should be requested or alternative procedures should be performed. When evaluating a SAS 70 report for its adequacy for reliance, the assessment team should consider the following:

> **Type I or Type II report –** A Type I report covers only the suitability of the controls' **design**, whereas a Type II report also assesses whether the controls are **operating effectively** (i.e., the controls are tested by the service organization's auditor). Because OMB Circular A-123 requires management to assess the design **and** operating effectiveness of its internal control over financial reporting, a Type I report cannot be used for the assessment team's assessment to support operating effectiveness.

Considerations regarding Annual Assurance Statements and SAS 70s

Scope of the review – The report must cover the processes and controls relevant to the assessment team's assessment process. To ensure that this objective is met, the assessment team should collaborate with its service organization to determine the scope of the Annual Assurance Statement or SAS 70 report. These reports should cover (1) the relevant information processing objectives/CAVR that are addressed at the service organization and (2) the general computer controls for any applications relevant to the assessment team's assessment process.

Some service organizations have multiple processing sites. The assessment team must ensure that the processing location responsible for providing its services is covered by the report. If not, additional procedures will be required.

User controls – In most situations, to conclude that effective internal control over financial reporting exists, the assessment team must demonstrate effective controls at both the organization and the service organization. The organization's controls over the service organization are referred to as "user controls" and are typically documented in the Annual Assurance Statement or SAS 70 report. The assessment team should evaluate and test these controls. For example, the integrity of outsourced payroll processing will depend on the integrity of the inputs from the organization, including information relating to new employee, terminations, and salary increases. If the organization is responsible for providing this information to the service organization, the user controls vis-à-vis this information will be important to ensure the overall integrity of the payroll-processing output from the service organization.

Period of time covered – The assessment team must consider the period of time covered by the Annual Assurance Statement or Type II SAS 70 report. A report dated earlier than six months prior to the organization's fiscal year-end date would result in limited benefits because of the extent of additional procedures that would be necessary. However, if a report's date is too close to year-end, the assessment team may be unable to obtain the report in sufficient time to allow for evaluation and remediation.

As the intervening period between the date of the Annual Assurance Statement or SAS 70 report and the year-end of the organization increases, the assessment team should consider update procedures. The assessment team should consider whether, during the intervening period, there have been any:

- Changes in personnel with whom management interacts at the service organization;
- Changes in reports or other data received from the service organization;
- Changes in contracts or service level agreements with the service organization; and
- An error in the service organization's processing.

Based upon these considerations and the significance of the services to the organization, the assessment team should determine the extent of any further procedures.

Opinion – The assessment team should determine if the cross servicing organization's or service auditor's opinion is unqualified (i.e., in the auditor's opinion, the service organization's controls are designed effectively and are operating as designed). If the opinion is qualified, the assessment team should assess the nature of the internal control deficiencies and their impact on the organization's internal control over financial reporting. In this case, the assessment team may need to perform additional procedures to obtain assurance over the service organization's controls or request that the service organization remediate the internal control deficiencies prior to its fiscal year-end. The assessment team can rely on a SAS 70 report that is issued by its external auditor, as long as management did not engage its external auditors to perform the SAS 70 audit at the service organization.

Testing Exceptions – Although the cross servicing organization or service auditor may have issued an unqualified opinion, exceptions in testing may exist. The assessment team should evaluate the implications of these exceptions in the area that is being tested (nature, extent, and risk) as it would if exceptions to an internal process were identified.

Additional Procedures – The Department believes that in some cases, an Annual Assurance Statement or a Type II SAS 70 report will not be sufficient for the assessment team's assessment of internal control over financial reporting. For example, if an organization outsources substantially all general-ledger and transaction-processing functions to a service organization, the organization may conclude that an Annual Assurance Statement or a Type II SAS 70 report would not provide sufficient evidence of operating effectiveness due to the significance of the outsourced processes. In this situation, the assessment team should assess whether additional procedures need to be performed to evaluate the design and operating effectiveness of the service organization's controls. Conversely, if a service organization performs routine payroll processing for many customers, it is likely that the service organization's clients would conclude that an Annual Assurance Statement or a Type II SAS 70 report sufficiently assesses the design and operating effectiveness of the service organization's controls.

Documentation – All key decisions made regarding service organizations and the use of assurance statements and SAS 70s should be documented as part of the planning phase. Assurance statements and SAS 70s that are received from service organization should be retained as part of the assessment teams documentation as described in Section Four – Documentation. The assessment team does not need to document processes that occur at the service organization, but does need to document how user controls are performed within the agency. User controls would need to be tested as part of the testing phase of management's assessment.

Point of Focus 8

Service Organization Timing

Obtaining an Annual Assurance Statement from a cross-servicing Component or a Type II SAS 70 report from a federal, state, or commercial entity for the first time can be a lengthy process. The service organization may need to remediate certain processes, and thus it often takes six months to a year to obtain a final report after a request is made. Accordingly, agencies using commercial service organizations should make this determination as soon as possible.

Furthermore, a great deal of coordination between DHS's Components will be required, so the management of each Component will be able to determine its overall control effectiveness.

3.7.4 – Step 7d – If an Annual Assurance Statement or SAS 70 does not exist, determine alternative procedures

If an Annual Assurance Statement or Type II SAS 70 report cannot be obtained, or the report obtained does not adequately address the information processing objectives/CAVR required by the assessment team, alternative procedures should be performed over the service organization's internal control. These procedures may include one or more of the following:

- Perform tests of controls at the service organization;
- Obtain a report on the application of agreed upon procedures that describes the tests of relevant controls; and
- Perform tests of the user controls over the activities of the service organization.

Perform tests of controls at the service organization

If the organization's contract with the service organization has a "right to audit" clause or the organization is otherwise permitted by the service organization to perform an audit, the assessment team may have its own personnel review and test the controls at the service organization. This review would be similar to the assessment that the assessment team would perform on its internal processes. The review would need to cover the control activities at the service organization, as well as any relevant controls covering the other four Components of internal control (including general computer controls).

Obtain a report on the application of agreed upon procedures that describes the tests of relevant controls

An agreed-upon procedures report may be used if it provides a level of evidence similar to a SAS 70 report[25]. If an agreed-upon procedures report is to be relied upon, the assessment team should consider the following factors:

- The service organization's controls that (1) are relevant to the organization's internal control over financial reporting and (2) cover all five Components of internal control (including general computer controls).

[25] PCAOB AS 2.

- The time period covered and the nature and results of the tests that the service auditor applied to the service organization's controls to validate that they are operating effectively.

Perform tests of the user controls over the activities of the service organization

The assessment team should assess whether its user controls would provide adequate assurance by considering whether (1) a breakdown of control at the service organization could lead to a misstatement that is more than inconsequential and (2) management's user controls would detect or prevent the misstatement in a timely manner.

For example, assume that an entity uses a service organization to process payroll. On one occasion, the service organization erroneously inputs the wrong payment amount for a new employee, causing the overall payroll amount to be incorrect. If management performs an independent review of the total amount that was paid at every pay period, the error would be detected, researched, and resolved before the error was recorded in the organization's financial records. In this case, the assessment team may be able to rely on its own user controls.

User controls may take the form of:

Input/Output Controls - In most outsourcing situations, the entity will have some access to the information processed by a service organization. In some cases, this information may enable the organization to fully reconcile the service organization's results with the results of an independent source. For example, an entity using a payroll service organization could compare the data submitted to the service organization with reports or information received from the service organization after the data has been processed. The entity also could recompute a sample of the payroll amounts for clerical accuracy and review the total amount of the payroll for reasonableness.

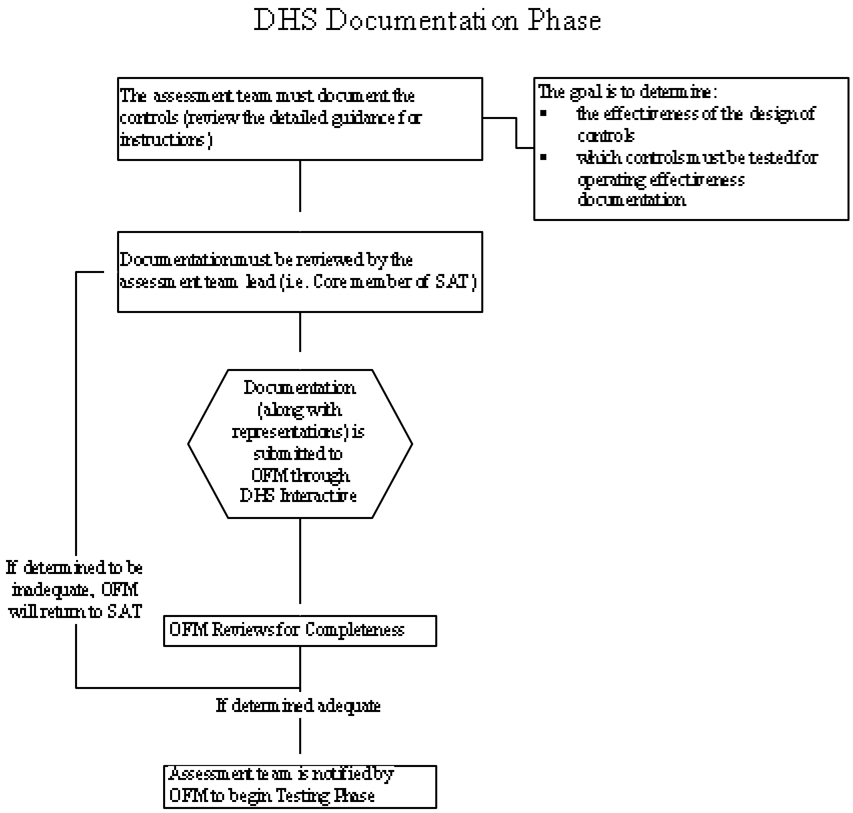
Performance Monitoring - Management may have a process for monitoring the service organization's performance in relation to various metrics, as typically defined in a service level agreement. Most of these metrics will be tailored to specific operations. In some situations, however, such monitoring may provide some indirect assurance that the service organization's controls are operating properly. For example, management may regularly review the security, availability, and processing integrity of service level agreements and related contracts with third-party service organizations. A designated individual would be responsible for regularly monitoring the third party's performance and reporting whether that performance meets certain criteria.

Process Controls - In some outsourcing situations, the entity's user controls may be closely tied to the service organization's processes and provide direct assurance over their operation. For example, an entity that has outsourced its IT development to a service organization may choose to document, track, approve, and test all application changes internally, thus retaining significant control over the IT development process.

Typically, the assessment team's testing of its user controls that pertain to a service organization is not as effective as the assessment team's testing of controls that are in place at the service organization itself. Accordingly, the assessment team should determine whether an assessment of the organization's user controls alone is sufficient to establish the reliability of the relevant information processing objectives/CAVR. The assessment team may rely solely on testing its own user controls in situations where (1) such controls cover all relevant assertions over the accounts and disclosures affected by the outsourced processes and (2) the significance and risk of processing at the service organization to the overall user organization's financial statements is low.

SECTION FOUR: Documentation Phase

Figure 14: Overview: The Documentation Phase


DHS Documentation Phase
The assessment team must document the controls (review the detailed guidance for instructions)
The goal is to determine:
▪ the effectiveness of the design of controls
▪ which controls must be tested for operating effectiveness documentation
Documentation must be reviewed by the assessment team lead (i.e. Core member of SAT)
Documentation (along with representations) is submitted to OFM through DHS Interactive
If determined to be inadequate, OFM will return to SAT
OFM Reviews for Completeness
If determined adequate
Assessment team is notified by OFM to begin Testing Phase

Purpose and Scope

The Documentation Phase section describes the required documentation for the project. The documentation produced in the internal control assessment project forms the basis and support for management's evaluation of internal control over financial reporting. Further, OMB Circular A-123, Appendix A requires the Senior Assessment Team to document its understanding of the agency's internal control over financial reporting[26]. At each Component this responsibility falls under the Component Assessment Team (referred to as the "assessment team") headed by a core member of the Senior Assessment Team.

The Component Assessment Teams will determine the scope of documentation, prepare walkthroughs for each process, develop control documentation, and document their assessment of the design and operational effectiveness of controls.

The assessment team documentation should support its:

- Approach and planning decisions;
- Evaluation of whether the organization's system of internal control is designed to prevent or detect material misstatements;
- Conclusion that the tests of operating effectiveness were appropriately planned and performed; and
- Consideration of the test results when determining assurance.

In addition, OMB Circular A-123, Appendix A requires documentation of the following:

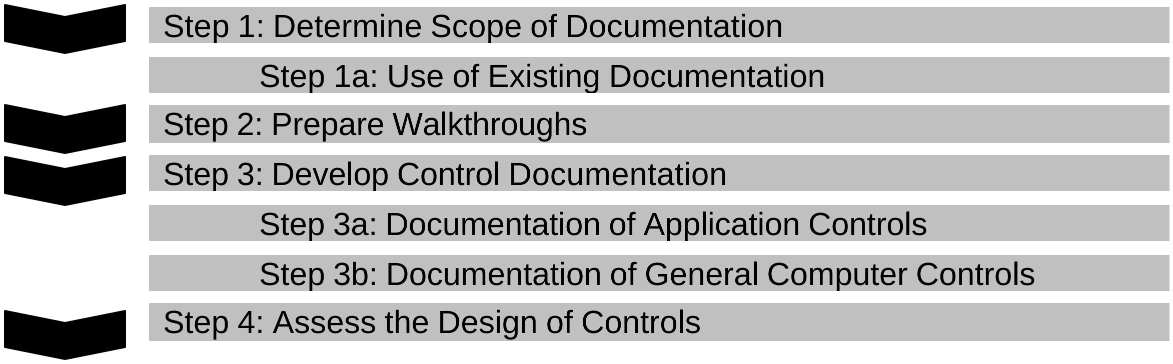
- The establishment of assessment teams, its authority and members;

[26] OMB Circular A-123 Management Responsibility for Internal Control, Appendix A page 28.

- Contracting actions if contractors are used to perform or assist in the assessment;
- Communications with agency management and employees regarding the assessment; and
- Key decisions of the assessment teams.

Once the assessment team has documented the Component's controls (Refer to documentation steps below), the documentation must be reviewed by the assessment team lead. The documentation along with appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls must be submitted to OFM electronically via the Department's intranet site at https://interactive.dhs.gov, within the specified timeframe. OFM will review the documentation for completeness. If OFM finds the documentation to be inadequate, it will notify the assessment team lead. The notification will include areas for improvement or where clarification is needed. The assessment team must re-submit the specified documentation within the deadlines established by OFM. Once approved, OFM will notify the assessment team to begin the next phase of the assessment.

To meet its responsibility, the assessment team must follow the following four documentation steps when documenting its internal control:



Step 1: Determine Scope of Documentation

Step 1a: Use of Existing Documentation

Step 2: Prepare Walkthroughs

Step 3: Develop Control Documentation

Step 3a: Documentation of Application Controls

Step 3b: Documentation of General Computer Controls

Step 4: Assess the Design of Controls

4.1 – Step 1: Determine Scope of Documentation

The assessment team should document the controls related to significant line items and related accounts, disclosures, and processes (including transactions and systems) at the locations that fall within the scope of the project (in-scope processes), as described in Section Three, Planning. Such locations include:

- Individually important locations;
- Locations that are not individually important but pose specific risks that make them important; and
- Locations that are not individually important but that could be important when aggregated with other locations or business units.

In addition, management should have at least a minimum level of documentation of controls at locations that are not considered significant, either individually or in the aggregate.

4.1.1. - Step 1a: Use of Existing Documentation

Before commencing the documentation process, the assessment team must inventory existing documentation as documentation may already exist as part of normal agency policy or procedure. If the assessment plans to rely on existing documentation, it must:

- Ensure the documentation includes the requirements described above;
- Ensure the documentation is current;
- Ensure the documentation is presented in a format that facilitates the assessment process; and
- Separately identify, verify, validate and maintain the documentation it uses in making its assessment.

The documentation prepared by internal or external auditors may also be used, but the assessment team must take responsibility for verification and maintenance of that documentation.

4.2 – Step 2: Prepare Walkthroughs

The assessment team should prepare walkthroughs documenting the processes related to significant line items and related accounts and disclosures including related transactions and systems. The documentation must cover more than just the controls that the assessment team plans to test. Documentation must enable management to understand the processes underlying the significant line item from beginning to end covering the initiation, authorization, recording, processing, and reporting of individual transactions. In addition, documentation must:

- Identify the cycle transactions, each significant accounting application, and each significant financial management system included in the cycle,
- Describe interfaces with other cycles,
- Identify financial statement line items and general ledger accounts included in the cycle,
- Describe the operating policies and procedures relating to the processing of cycle,
- Identify and describe significant provisions of laws and regulations (e.g., the process used by management to ensure compliance with laws and regulations such as the Antideficiency Act),
- Describe performance measures used by management to ensure operational controls are in place (e.g., use of suspense and clearing accounts for Fund Balances with Treasury, delinquent accounts receivable, EFT Payments, prompt pay statistics, etc.), and
- Describe relationships to other financial reporting processes.

Documentation of processes must be in the form of flowcharts supplemented by narrative descriptions.

Refer to Appendix Q for an example walkthrough narrative and Appendix J for guidelines on flowcharts.

4.3 – Step 3: Develop Control Documentation

Once the assessment team has prepared walkthroughs related to the in-scope processes, it should prepare control evaluations for each significant line item including its related accounts, disclosures and processes that align specific controls with information processing objectives/CAVR and financial statement assertions. Related transactions and systems must also be included in the control evaluation. The control evaluations should include documentation of the design of the controls that are relevant to financial reporting. Controls over effectiveness and efficiency of operations and compliance with laws and regulations that have a direct and material effect over financial reporting must be included in the control evaluations. Documentation related to the design should include a description of controls over the prevention and detection of fraud, including who performs the control and the related segregation of duties.

Point of Focus 9

The assessment team's documentation of the design of controls should be sufficiently detailed to allow a person who knows little about the process to understand and evaluate whether the controls are designed effectively, enabling that person to create a test plan. A lack of documentation limits the ability of management to properly communicate the control processes throughout the organization and properly monitor internal control.

Control evaluations should break down each process into sub-processes, all of which should address information processing objectives/CAVR and ultimately, the relevant financial statement assertions. Documentation of control activities should, at a minimum, provide answers to the following questions:

1. ***What** is the risk being controlled?*
2. ***What** is the control activity?*
3. ***Why** is the activity performed?*
4. ***Who** (or what system) performs the control activity?*
5. ***When** (how often) is the activity performed?*
6. ***What** mechanism is used to perform the activity (reports and systems)?*

Control evaluations provide a rigorous framework that ensures all relevant controls are adequately documented, and it also provides a structured mechanism for identifying control deficiencies. Without control evaluations, it would be difficult to identify (1) control gaps, and (2) the controls covering all relevant information processing objectives/CAVR or financial statement assertions. This documentation allows management to assess whether the controls cover the financial statement assertions that were mapped to each account during the planning phase.

Refer to Appendix K for the Control Evaluation Template.

4.3.1 –Step 3a: Documentation of Application Controls

Application controls should be identified and documented using the same control evaluation documentation procedures as are used for the rest of the controls within the operating cycle. Controls should be documented to help ensure that each transaction processed by the application is complete, accurate, valid, and appropriately accessed (restricted access). Because application-level controls are tied to the organization's process controls more closely than general computer controls, responsibility for documenting and assessing application-level controls should rest with the individuals (or teams) responsible for the related operating process.

The GAO is in the process of developing Chapter 4 of the FISCAM "Evaluating and Testing Application Controls," which will aid the assessment team in documenting and assessing application controls. A specific methodology like this can be helpful when documenting those application controls which may not appear to be as tightly coupled with the process/cycle; for example, master files that are used to help identify unauthorized transactions and programs that perform limit and reasonableness checks on critical calculations. However, until these guidelines are finalized and released, the Department suggests that the assessment team use the information processing objectives/CAVR as noted above.

The following table is an overview of what must be documented for each FISCAM domain and the linkage to each financial statement assertion.

Figure 15: Overview – Documentation by Domain

Domain	What Must be Documented?	Financial Statement Assertions Affected
Information Technology Control Environment	Each information technology organization deemed to be in-scope	All
Program Development	Significant development projects underway	All
Program Changes	All in-scope applications and information technology environments	All
Access to Programs and Data (Security)	All in-scope applications and information technology environments	All – but most relevant to completeness and existence
Computer Operations	All in-scope information technology environments	All – but most relevant to completeness

The assessment team should use the same methodology deployed for the other controls within a process to effectively document the application controls. Furthermore, application controls should be documented within the same control evaluation template (see Appendix K) as the rest of the controls related to its specific process/cycle.

4.3.2 – Step 3b: Documentation of General Computer Controls

An IT internal control framework will help organizations effectively identify and document their general computer controls. Several of these frameworks exist; however, the FISCAM was created by the General Accountability Office (GAO) as the primary tool to be used by agencies within the federal government to evaluate their general computer controls. The preface of FISCAM states:

> “Federal agencies, the Congress, and the public rely on computer-based information systems to carry out agency programs, manage federal resources, and report program costs and benefits. The methodology outlined in this manual provides guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of data maintained in these systems. The manual is primarily designed for evaluations of general and application controls over financial information systems that support agency business operation…We expect that the manual will serve as a common language between information system auditors and financial auditors so that they can effectively work together as a team, understand the tasks to be accomplished, and achieve common goals.”

Although FISCAM should be used to help an organization identify and document its general computer controls, each organization should carefully consider which of FISCAM’s “critical elements” (control objectives) and related “control activities” are relevant to its specific risks and unique IT environment. The organization may not need to include all control activities specified by FISCAM, or may need to include others not specified by FISCAM. The GAO’s *Standards for Internal Control in the Federal Government*, addresses the ever evolving control environment:

> “Because information technology changes rapidly, controls must evolve to remain effective. Changes in technology and its application to electronic commerce and expanding Internet applications will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility

> for data processing in the hands of the end users, the needed controls should be identified and implemented."

Accordingly, each organization should use judgment to tailor FISCAM, so it is appropriate to the size and complexity of the IT environment. The security categorization of information and information systems completed by the agency as a result of FIPS Publication 199 can help the organization appropriately tailor FISCAM. According to FIPS Publication 199, "the security categories [low, medium, and high] are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals." This security categorization is based on the following three security objectives: confidentiality, integrity, and availability.

Consulting other internal control frameworks such as the "Control Objectives for Information and related Technology" (CobiT) may also be helpful when determining the IT control objectives necessary for your organization. Note: CobiT includes many control objectives that are not relevant to achieving the financial statement assertions. Ultimately, management should identify the appropriate control objectives and then determine if the necessary controls are in place to meet these objectives.

The following table is an overview of what must be documented for each of the major categories of FISCAM and how the financial statement assertions link to each of these categories.

Figure 16: Overview – Documentation by FISCAM Category

FISCAM Category	What Must be Documented?	Financial Statement Assertions Affected
Entity-wide Security Program Planning and Management (SP), FISCAM Section 3.1	The design of the entity-wide security controls pertaining to all in-scope applications and IT environments. (Note: As indicated in Section 3, the in-scope applications are those that play a role within the processes/cycles that are considered significant to the financial statements).	All
Access Control (AC), FISCAM Section 3.2	The design of the access controls pertaining to all in-scope applications and IT environments.	All – but most relevant to completeness and existence
Application Software Development and Change Control (CC), FISCAM Section 3.3	The design of the application software development controls pertaining to significant development projects underway (Software Development). The design of the change controls pertaining to all in-scope applications and IT environments (Change Control).	All
System Software (SS), FISCAM Section 3.4	The design of the system software controls pertaining to the computer platforms hosting the in-scope applications and other systems connected to those platforms.	All
Segregation of Duties (SD), FISCAM Section 3.5	The design of the segregation of duties controls pertaining to all in-scope applications and IT environments.	All

FISCAM Category	What Must be Documented?	Financial Statement Assertions Affected
Service Continuity (SC), FISCAM Section 3.6	The design of the service continuity controls pertaining to all in-scope applications and IT environments.	All – but most relevant to completeness and existence

Because general computer controls are pervasive controls, they cannot be tied to any one specific process/cycle. As a result, general computer controls should be documented in their own evaluation templates, which are categorized by FISCAM area. An example of a general computer control evaluation template using FISCAM terminology is included in Appendix L (Sample General Computer Control Matrix).

Point of Focus 10

Leverage Common Elements of Information Technology

In large IT organizations, there are generally common processes across IT organizations supporting different business units or geographies. In these cases, separate control evaluations for each application or IT environment may not be necessary. A common control evaluation, documenting the standard process, can be developed. Exceptions to this standard process may then be documented in a matrix specific to an application or environment. For example, the organization may have a common program change process across several applications. If this is the case, a generic control evaluation covering the standard process can be developed and the control activities documented.

4.4 – Step 4: Assess the Design of Controls

In assessing the design of controls, the assessment team must determine whether the controls (procedures, processes, policies, and systems) will, if operating as intended, provide reasonable assurance that management's information processing objectives/CAVR are being met in relation to the relevant financial statement assertions for all significant accounts and disclosures (often referred to as design effectiveness). The assessment team will evaluate the operating effectiveness of controls during the testing phase of the project. However, if the design of a control is flawed, the entity will not achieve the desired assurance that the control is capable of preventing or detecting a misstatement even if the control is operating as intended. Management will need to remedy design deficiencies.

After the assessment team has documented the design of the controls for the in-scope processes, it must determine (1) the effectiveness of the design of controls and (2) which controls must be tested for operating effectiveness. These two steps are closely linked; however, they will be presented sequentially for ease of discussion.

Documentation of the assessment should be retained for seven years, consistent with the requirement of the independent public accountant[27]

Effectiveness of the Design of Controls

The evaluation of design effectiveness addresses whether the system of internal control is suitably designed to prevent or detect on a timely basis, material misstatements in significant accounts and disclosures. This evaluation should cover (1) persuasive entity-level controls (management should assess the internal control

[27] Current requirement based on PCAOB AS2

Components of control environment, risk assessment, information and communication, and monitoring) and (2) specific transaction-level control activities related to all relevant assertions for all in-scope processes. When assessing design effectiveness, the assessment team should focus on:

- The alignment between the controls and the risks identified (i.e., whether the processes and related controls appear to be effective in achieving management's stated objectives and managing its risks). The appropriateness of a control alignment relates to the control's directness and selectivity.
  - **Directness**: The more direct the alignment/relationship, the more effective the control may be in achieving the objective. For example, management reviews of inventory reports that summarize the inventory by storage facility may be less effective in preventing or detecting misstatements in the existence assertion for inventory than a periodic physical inventory, which is more directly related to the existence assertion.[28]
  - **Selectivity**: Refers to the magnitude of the amount, or the significance of other criteria or distinguishing characteristics, that a specific control will identify as an exception condition. Examples of selectivity thresholds are (1) a requirement for additional approvals of all payments to vendors in excess of $25,000 and (2) management reviews of all payments to vendors not on an entity's approved vendor list. When determining whether a control is likely to be effective, the assessment team should consider the likelihood that items that do not meet the selectivity threshold could, in the aggregate, result in material misstatements of financial statements, material non-compliance with budget authority, material non-compliance with significant provisions of laws and regulations, or significant ineffective or inefficient use of resources. The assessment team also should consider the appropriateness of the specified criteria used to identify items on a management or exception report. For example, information systems input controls (such as the matching of vendor invoices with receiving reports and purchase orders) that require exact matches of data from different sources before a transaction is accepted for processing may be more effective than controls that accept transactions that fall within a broader range of values. On the other hand, controls based on exception reports that are limited to selected information or use more selective criteria may be more effective than lengthy reports that contain excessive information[29].
- Whether the controls satisfy the information processing objectives/CAVR and the relevant financial statement assertions.
  - To be considered effective, the combination of identified automated controls (or a combination of controls) for a specific sub-process, should address all information processing objectives/CAVR and the related financial statement assertions.
- Frequency of the control – whether the control will detect or prevent the risk identified on a timely basis (i.e., in some cases, a detective control may be adequate, but in other cases, an entity should ensure adequate preventative controls are in place).

[28] Based on the GAO/PCIE Financial Audit Manual, section 340.

[29] Ibid

  - The regularity with which controls are applied can determine the effectiveness of the control. Generally, the more frequently a control is applied, the greater the likelihood that it will be effective[30].

- Knowledge and experience of the people involved in performing the controls.
  - The person applying a control must have the necessary knowledge and expertise to properly apply it. The lesser the person's experience and skills, the less likely that the control will be effective (i.e., effectively applied). Also, the effective application of a control is generally adversely affected if the activity (1) is performed by an employee who has an excessive volume of work or (2) is not performed carefully[31].

- Segregation of duties relevant to the process being controlled.
  - Lack of segregation of duties over control activities and monitoring controls hinders the effectiveness of the control. For example, an effectively design control activity such as a reconciliation of Fund Balance with Treasury to Treasury records must be considered ineffective if the related monitoring activity of supervisory review of the reconciliations is performed by the same person.

- Timeliness in addressing issues and exceptions that result from the control activity (Follow-Up Procedures).
  - A control's effectiveness is dependent on the effectiveness of follow-up procedures. To be effective, these procedures should be applied on a timely basis and should (1) determine whether control exceptions represent misstatements and (2) correct all misstatements noted. For example, as a control, an accounting system may identify and put exception transactions into a suspense file or account. Lack of timely follow-up procedures to (1) reconcile and review the suspense file or account and (2) correct items in the suspense file or account would render the control ineffective[32].

- Reliability of the information used in the performance of the control.
  - If the control is contingent upon specified data, the reliability of the information will determine the effectiveness of the control. For example, if one of the controls over compliance with the Prompt Pay Act requires management to review a system derived management information report that ages receipt of invoices, the control will be rendered ineffective if the controls over the system (General or Application controls) used to produce the management information report are determined to be ineffective (i.e. unreliable).

- Period covered by the control.
  - To be effective the controls must be in place during the period under assessment.

Not all controls provide the same level of assurance. In evaluating the level of assurance provided by a given control, management should consider the nature of the control, how the control is applied, the consistency with

[30] Ibid

[31] Ibid

[32] Ibid

which it is applied, and who applies it. The degree of assurance over internal control will vary based on several factors, including those listed below:

Figure 17: Factors Affecting the Degree of Assurance over Internal Control

Less Assurance	Greater Assurance
Manual control	Automated control
Complex control (requires many steps, multiple calculations, etc.)	Simple control (single step, single calculations, etc.)
Control is performed by a junior, inexperienced person	Control is performed by an experienced manager
Detective control (detects a potential problem after a transaction is executed)	Preventive control (prevents a problem)
Single control	Multiple, overlapping controls
High-level control (analytics)	Detailed, transaction-level control
Control uses sampling	Control involves checking all items
Control takes place well after the transaction	Control occurs in real time (i.e., as the transaction takes place)

Management's evaluation of design effectiveness is important because only properly designed controls can mitigate risk. Thus, management should document its evaluation in a clear and comprehensive manner.

Point of Focus 11

An assessment of the control design should identify controls as effective, moderately effective, or not effective[33].

Controls to Test for Operating Effectiveness

Once the assessment team has made an assessment of the control design (i.e., effective, moderate effective, or not effective), the assessment team must determine and document which controls will be tested for operating effectiveness. For those controls whose design is deemed effective or moderately effective, the assessment team should test those controls to determine the extent to which the controls were applied, the consistency of their application, and who applied them.

If a control over an in-scope process is missing or its design is determined to be not effective considering the associated risk of error, the assessment team does not need to test this control for the purpose of concluding on control effectiveness. This instance should be noted in the report of deficiencies and suggestions for improvement. However, management may nevertheless seek to further test affected transactions to determine if there was any actual loss, fraud, waste, abuse, error, improper payment, or noncompliance resulting from those ineffective controls.

[33] OMB Circular A-123: Management Responsibility for Internal Control, Appendix A, page 27

The assessment team must test controls for all relevant financial statement assertions for all significant accounts, disclosures, and related processes, for all individually important locations and significant specific risks. Although one control may cover a specific assertion, the combination of preventive and detective controls is generally more effective[34].

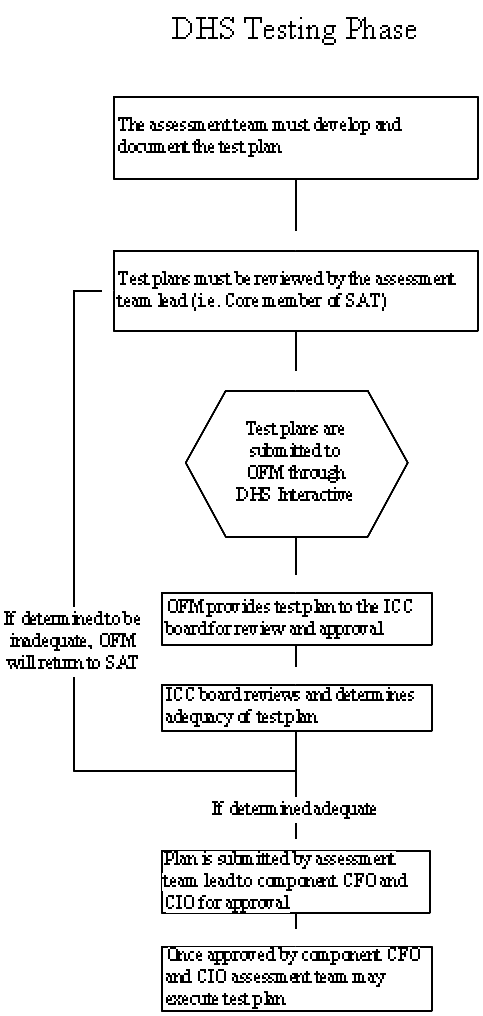
Controls whose design is deemed effective or moderately effective are considered “key controls” for simplicity. In this guide, we refer to controls that ultimately will be tested for operating effectiveness as key controls.

[34] PCAOB AS 2.

SECTION FIVE: Testing Phase

Purpose and Scope

Figure 18: Overview: The Testing Phase


DHS Testing Phase
The assessment team must develop and document the test plan
Test plans must be reviewed by the assessment team lead (i.e. Core member of SAT)
Test plans are submitted to OFM through DHS Interactive
OFM provides test plan to the ICC board for review and approval
ICC board reviews and determines adequacy of test plan
If determined to be inadequate, OFM will return to SAT
If determined adequate
Plan is submitted by assessment team lead to component CFO and CIO for approval
Once approved by component CFO and CIO assessment team may execute test plan

The Testing Phase section discusses what is required to test controls that are effectively designed. Controls are tested to ensure they are functioning properly. Testing is also necessary to support management assertion of the controls. This requires testing the controls, which must include each of the five Components of internal control over all relevant assertions for all significant line items and related accounts, and disclosures at each individually important location and over the specific risk areas at other locations. The assessment teams must retain evidence of this testing to support management's assessment of internal control over financial reporting.

The Component assessment team will prepare a test plan which details the assessment team's philosophy and approach to the testing phase (See steps below). The detailed test plan includes identification of controls to be tested, coordination and assignment of testing procedures, and a plan for test execution. The execution plan should identify how to test the controls, how to document and evaluate the results, and identify deficiencies. Once a plan is in place, testing is executed.

Once developed, the test plan must be presented to the Component's assessment team lead for validation and approval. Once approved by the assessment lead, the test plan must be submitted to OFM electronically via the Department's intranet site at https://interactive.dhs.gov, within the specified timeframe. OFM will provide the Component's plan to the ICC board for approval. If the ICC board finds the plan to be inadequate, OFM will notify the assessment team lead. The notification will include areas for improvement or where clarification is needed. The assessment team must re-submit the plan within the deadlines established by OFM. Once approved by the ICC board, the assessment team must provide the plans for approval to the Component CFO and CIO. Once approved by the Component CFO and CIO, the assessment team may begin the next phase of the assessment. Refer to Appendix U for a Testing Plan Template that covers the six steps.

Testing will require a significant effort. The assessment team should not underestimate the amount of time required and the complexities that will be encountered during the testing phase of the project. An organization-wide training effort will ensure all key personnel have the necessary skills to perform their portion of management's assessment. If a Component determines that they do not have the number of personnel with the necessary skill sets to perform the assessment they may need to consider the use of contractors.

The assessment team's assessment of the effectiveness of internal control over financial reporting is expressed at the level of reasonable assurance. The concept of reasonable assurance is built into the definition of internal control over financial reporting. Reasonable assurance includes understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. The cost of absolute assurance would be prohibitive. Reasonable assurance is the level that fulfils professional standards while producing a positive cost/benefit relationship. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance[35].

To obtain a high level of assurance, the assessment team must obtain sufficient competent evidence about the design and operating effectiveness of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements at each individually important location.

The testing plan is divided into six steps:

Step 1: Identify the Controls to be Tested

Step 2: Avoid Duplication of Efforts with Other Similar Activities

Step 3: Identify who will perform the Testing

Step 4: Develop and Execute the Test Plan

Step 5: Document Test Results

Step 6: Evaluate Test Results

These steps typically will be performed sequentially, but some aspects will be iterative as the results of testing necessitate changes in the plan or the need for retesting of remediated items. These steps should be described in the Component's overall testing plan.

5.1 – Step 1: Identify the Controls to Be Tested

The assessment team must demonstrate that controls covering all five Components of internal control are operating effectively relative to all significant line items and related accounts, disclosures, processes, and location. The nature of tests of control activities is typically more straightforward than the tests to be performed for the other Components of internal control. Evaluating the effectiveness of controls related to the control environment, risk assessment, information and communication, and monitoring Components typically requires greater judgment and qualitative analysis than is required for an evaluation of control activities.

The location selected and the testing performed should follow from the decisions made during the planning and documentation phases of the project, as reiterated below:

[35] GAO Standards for Internal Control in the Federal Government (GAO Green Book), pg 6

Figure 19: Selecting Locations and Tests to Perform

Category	Minimum Account Balance Coverage	Location/Operating Unit	Planned Procedures
1	60 – 70%	Individually important location and line items with specific risks	The ICC (at the consolidated level) and the assessment teams (at the Component level) will determine individually important locations and line items with specific risks. The assessment team will be required to perform detailed evaluation and tests of controls over significant (or "specific risk") accounts and disclosures at that location and testing of entity-level controls.
2	25 – 35%	Locations considered important when aggregated	The ICC (at the consolidated level) and the assessment teams (at the Component level) will determine locations considered important when aggregated. The ICC (at the Department-wide level) and the assessment teams (at the Component level) will be required to evaluate and test entity-level controls, if applicable, and consider obtaining other evidence or perform some tests of controls at locations if entity-level controls do not exist.
3	<5%	Immaterial location, individually and in the aggregate	The ICC (at the consolidated level) and the assessment teams (at the Component level) will determine immaterial locations, individually and in aggregate. No testing required by the assessment team.

For category 1 locations, testing would include transaction-level controls over the significant accounts and processes and entity-level controls. For category 3 locations, no specific control testing is required. For category 2 locations, if entity-level controls are in place, the assessment team should document and test them to evaluate whether they are operating effectively. For example, to determine whether an accounting manual's policies are implemented (an entity-level control); management will have to perform testing at selected individual locations in category 2 to determine whether local personnel have applied the policies in accordance with the accounting manual. The assessment team also may decide to obtain evidence about the operating effectiveness of control activities at these locations through other means, such as self-assessments, reviews by a quality assurance or internal control organizational unit, and monitoring controls.

The following table presents the minimum number of category 2 locations that should be subject to testing of entity-level controls.

Figure 20: Minimum Number of Locations

Number of Locations/operating units	Number of Locations to Test Entity-Level Controls
Less than 20	2 – 4
20 – 49	4 – 6
50 – 100	6 – 10
100+	10 – 20+

If entity-level controls cannot be relied upon for category 2 locations, detail testing of controls over significant line items and related accounts and disclosures will need to be performed.

5.2 – Step 2: Avoid Duplication of Efforts with Other Similar Activities

While the auditor's evidence of operating effectiveness will generally come from traditional testing (i.e., select a sample and reperform the control), the assessment team has more latitude in how it obtains the necessary evidence. For example, the assessment team may be able to obtain evidence of design and operating effectiveness through a objective self-assessment process, reviews by quality control or internal control organizational unit, or ongoing monitoring activities.

The assessment team should avoid duplicating reviews which assess internal control, and should coordinate its efforts with other evaluations to the extent practicable. For example, agencies are required to perform reviews of financial systems under FFMIA or information security under FISMA. Reviews performed by management, or at management's discretion, may be used to help accomplish this assessment. This is not to suggest that the assessment team can avoid sampling and testing of key controls. Rather, the assessment team can use alternative sources of evidence (if available) in combination with detailed sample testing to achieve a high level of assurance.

In developing its testing plan, the assessment team will need to consider whether it has sources of evidence beyond what it will obtain from detailed sample testing. Where the assessment team concludes such evidence exists, it may decide to reduce the sample sizes below what the auditor concludes is necessary to achieve a high level of assurance. In those cases, the assessment team should use sample sizes that when combined with other tests performed (i.e., self-assessment, etc.) would result in the total number of items tested to evaluate the operating effectiveness of a key control to be at least equal to the minimum sample sizes presented on figure 22. If the assessment team does not have other sources of evidence available, sample sizes used by the assessment team should be more than the minimum sample sizes presented on figure 22 when 1) an individual control is the sole control related to one or more financial statement assertion for a significant account or disclosure, 2) a control is considered to be more important, or 3) a higher level of assurance is required. Robust testing by the assessment team can significantly reduce the risk of a reportable condition or a material weakness being identified too late for remediation to occur prior to year-end[36].

[36] OMB Circular A-123, pg 13

The assessment team may consult with the agency IG to plan and coordinate related work. The IG may be involved in a consulting capacity, but shall not conduct management's assessment of internal control over financial reporting[37].

Possible sources of other testing may come from:[38]

- Management reviews conducted (i) expressly for the purpose of assessing internal control, or (ii) for other purposes with an assessment of internal control as a by-product of the review;
- Program evaluations;
- Reviews of financial systems which consider whether the requirements of FFMIA and OMB Circular No. A-127, Financial Management Systems are being met;
- Annual evaluations and reports pursuant to FISMA and OMB Circular No. A-130, Management of Federal Information Resources;
- Annual reviews and reports pursuant to IPIA to the extent they pertain to controls over financial reporting; and
- Type II SAS 70 report or annual assurance statement in the case where servicing is performed by the organization.

In all cases, the assessment team must take responsibility for the work which involves determining whether (1) the personnel who perform the work have the necessary competence and objectivity and (2) the procedures provide evidence sufficient to support the assessment. The assessment team has primary responsibility for assessing and monitoring controls, and should use other sources as a supplement to – not a replacement for – its own judgment.

5.3 – Step 3: Identify Who Will Perform the Testing

Once the assessment team has determined what controls are covered by another process, in full or in part, the assessment team must determine who will perform the remaining tests of controls.

The assessment team may evaluate the operating effectiveness based on procedures such as testing of controls by quality control or internal control organizational units, testing of controls by contractors under the direction of management, using service organization reports, inspecting evidence of the application of controls, or testing by means of a self-assessment process some of which might occur as part of management's ongoing monitoring process. In all cases, management must take responsibility for the work which involves determining whether (1) the personnel who perform the work have the necessary competence and objectivity (i.e. personnel performing the test should not be the person responsible for performing the control or report directly to the person performing the control); and (2) the procedures provide evidence sufficient to support management's assessment[39].

[37] OMB Circular A-123, pg 28

[38] OMB Circular A-123, pg 13

[39] PCAOB AS 2.

5.4 – Step 4: Develop and Execute the Test Plans

To facilitate review and approval by the various interested parties, formal test plans should document the key elements of the test and the results. Test plans should cover all controls that are selected for testing and should specify the following key elements:

- **Key controls to be tested –** The assessment team should summarize the controls to be tested at the financial statement assertion level.
- **Nature of tests to be used –** Tests should be categorized as inquiry, observation, examination, or reperformance.
- **Extent of testing –** The plans should specify the number of items that are to be tested and the method and reasons for selecting those items.
- **Timing of procedures –** The plans should specify when the testing should be performed and the time span that the tests cover, including update testing planned from the interim testing date to year-end.
- **Description of the test –** The plans should specify the procedures to be performed and the assertions supported.
- **Key administrative items –** The plans should identify who will perform the test, when the test will be performed, what evidence will be reviewed, and where the control is performed.
- **Documentation –** The plans should describe the source documentation required.
- **Exceptions –** The plans should describe how exceptions will be investigated and addressed and when additional testing should be performed.

See Appendix U for a Test Plan Template.

In many cases, a number of controls can be tested with a single sample of transactions that follows the financial process through a sequence of activities, which provides the tester an enhanced understanding of how various controls interact. For example, one technique for testing the controls in a procurement process is to select a sample of purchases. Authorization can be tested by validating the appropriate signatures on the contract. Accuracy of the prices can be verified by assessing whether modified prices (a) match what is specified in the contract and (b) were authorized.

Nature of Tests

The nature of tests can be classified into four categories: inquiry, observation, inspection, and reperformance. These categories are described below.

- **Inquiry**
  Inquiry tests are conducted by making either oral or written inquiries of entity personnel involved in the application of specific control activities to determine what they do or how they perform a specific control activity. Such inquiries are typically open-ended. Generally, evidence obtained through inquiry is the least reliable audit evidence and generally should be corroborated through other types of control tests (observation or inspection). Inquiry of a control’s effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively. The reliability of evidence obtained from inquiry depends on various factors, such as:

  - The competence, experience, knowledge, independence, and integrity of the person of whom the inquiry was made. The reliability of evidence is enhanced when the person possesses these attributes;
  - Whether the evidence was general or specific. Evidence that is specific is usually more reliable than evidence that is general;
  - The extent of corroborative evidence obtained. Evidence obtained from several entity personnel is usually more reliable than evidence obtained from only one; and
  - Whether the evidence was provided orally or in writing. Generally, evidence provided in writing is more reliable than evidence provided orally[40].

- **Observation**
  Observation tests are conducted by observing entity personnel actually performing control activities in the normal course of their duties. Observation generally provides highly reliable evidence that a control activity is properly applied when the assessment team is there to observe it; however, it provides no evidence that the control was in operation at any other time. Consequently, observation tests should be supplemented by corroborative evidence obtained from other tests (such as inquiry and inspection) about the operation of controls at other times. However, observation of the control provides a higher degree of assurance than inquiries, and may be an acceptable technique for assessing automated controls.[41]

- **Inspection**
  Inspection of evidence often is used to determine whether manual controls are being performed. Inspection tests are conducted by examining documents and records for evidence (such as the existence of initials or signatures) that a control activity was applied to those documents and records.

  System documentation, such as operations manuals, flow charts, and job descriptions, may provide evidence of control design but do not provide evidence that controls are actually operating and being applied consistently. To use system documentation as part of the evidence of effective control activities, the assessment team should obtain additional evidence on how the controls were applied.

  Since documentary evidence generally does not provide evidence concerning how effectively the control was applied, the assessment team generally should supplement inspection tests with observation and/or inquiry of persons applying the control. For example, the assessment team generally should supplement inspection of initials on documents with observation and/or inquiry of the individual(s) who initialed the documents to understand the procedures they followed before initialing the documents.[42]

- **Reperformance**
  It will normally be necessary for the assessment team to reperform controls to obtain sufficient evidence of its operating effectiveness. For example, a signature on a voucher package to indicate that the signer approved it does not necessarily mean that the person carefully reviewed the

[40] Definition adapted from the GAO/PCIE Financial Audit Manual, section 350

[41] Ibid

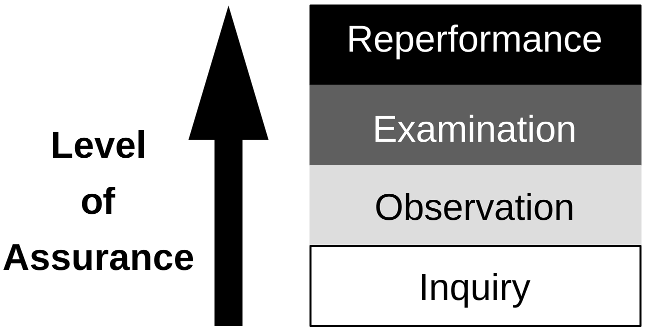
[42] Ibid

package before signing. The package may have been signed based on only a cursory review (or without any review). As a result, the quality of the evidence regarding the effective operation of the control might not be sufficiently persuasive. If that is the case, the assessment team should reperform the control (e.g., checking prices, extensions, and additions) as part of the test of the control. In addition, we might inquire of the person responsible for approving voucher packages what he or she looks for when approving packages and how many errors have been found within voucher packages. We also might inquire of supervisors whether they have any knowledge of errors that the person responsible for approving the voucher packages failed to detect. Because we are reperforming a control, it is not necessary to select high value items for testing or to select different types of transactions.

Combining two or more of these tests can provide greater assurance than using only one technique. The more significant the account, disclosure, or process and the more significant the risk, the more important it is to ensure that the evidence extends beyond one testing technique. The nature of the control also influences the nature of the tests of controls that should be performed. Most manual controls will be tested through a combination of inquiry, observation, examination or reperformance.

The relative level of assurance by nature of test is illustrated in the following chart:

Figure 21: Relative Level of Assurance by Nature of Test



Extent of Testing

The extent of testing of a particular control will vary depending on a variety of factors, including whether a control is automated or manual.

Testing of Automated Controls

For an automated control, the number of items tested can be minimal (one to a few items), assuming that IT general computer controls have been tested and found to be effective. A common automated control is an edit check that is activated during data entry. If letters were entered into a dollar value field, an error message would prevent the entry from being processed until corrected. Each attribute of the automated control should be tested for operating effectiveness. In this example, a few different invalid entries should be entered to demonstrate that the control is working effectively. In some cases, management override procedures may allow an automated control to be circumvented. This override capability should be evaluated to assess potential internal control deficiencies.

When testing automated controls, the assessment team must (1) ensure general computer controls are effective and (2) have performed a detailed review of the controls within the organization's computer applications (e.g., a pre-implementation or a post-implementation review). In the previous example, the assessment team should have developed a baseline understanding that the edit-check control is designed to work under all circumstances.

If management has never performed a detailed pre- or post-implementation review of the controls for the organization's computer applications or there are weak program change controls, it is the responsibility of the assessment team to ensure that the automated controls are working as designed. There are several ways to accomplish this objective, from the extreme of program code review to detailed walkthroughs ensuring all relevant logic paths are covered. For third-party software that has not been modified, the assessment team should validate that the standard configurations are appropriately set and ensure there is a control process over configurable parameters. For custom-developed or in-house applications, more extensive procedures to validate the design of the control may be required. However, if independent verification and validation (IV&V), testing of changes, has been performed for custom- or in-house developed programs, management should evaluate the level of reliance, if any, that can be placed on these IV&V procedures.

Point of Focus 12

Differentiating Between Manual and Automated Controls

In most cases, it will be clear whether a control is manual or automated. However, to novice testers this distinction can be confusing. A control may rely on an automated process, but the key Component of the control is manual. For example, a common control includes a systematic three-way match of receiving reports, purchase orders, and vendor invoices. The system automatically generates an exception report of unmatched items. The exceptions are then reviewed and cleared by the procurement Department. This control has two elements (1) the automated three-way match and (2) the manual review by the accounts payable Department. The automated and manual control elements must be evaluated separately using the appropriate test guidance.

Testing of Manual Controls

Tests of manual controls should include a mix of inquiry, observation, examination, or reperformance. Inquiry alone, however, does not provide sufficient evidence to support the operating effectiveness of a control. Effective testing will generally require examining a control at a particular location/operating unit in different instances (referred to as "sampling"). Inherent to sampling is the risk that although the assessment team may find nothing amiss in the samples (resulting in a conclusion that a control is operating effectively), the control is not necessarily operating effectively at all times. The assessment team should minimize this sampling risk by selecting an appropriate number of times to test (perhaps by considering the concepts of statistical sampling theory, although not necessarily applying statistical sampling). Sampling risk increases with the frequency of the control's activation. The extent of the assessment team's testing is based on its judgment and the level of assurance it expects to derive from the test. The following table should be used as a guide to support a conclusion that a manual control is operating effectively, provided no exceptions are found:

Figure 22: Manual Control Effectiveness – Sample Sizes

Frequency of Manual Control's Performance	Typical Number/Range of Times to Test Controls	Factors to Consider When Deciding the Extent of Testing
Annually	1	■ Complexity of the control ■ Significance of judgment in the control operation ■ Level of competence necessary to perform the control ■ Frequency of operation of the control ■ Impact of changes in volume or personnel performing the control ■ Importance of the control ● Addresses multiple assertions ● Period-end detective control ● Only control that covers a particular assertion
Quarterly	2	
Monthly	2 to 5	
Weekly	5 to 15	
Daily	20 to 40	
Multiple Times a Day	25 to 60	

The sample size that management decides to select for testing should be based on the significance of the control in question and the level of assurance desired. The fewer items tested, the greater the risk of an incorrect conclusion. Thus, for highly critical controls, or when a single manual control provides the sole support for a financial statement assertion regarding a significant account, the assessment team should consider increasing its sample size to the high end of the range provided in the table above. This decision should be made after considering other evidence available to the assessment team (e.g., results of self-assessment, testing by the OIG, or evidence from other monitoring controls). The combination of evidence should provide the assessment team with a high level of assurance the control is operating effectively. When no exceptions are found, these sample sizes will provide the assessment team with a high level of assurance that the control is operating effectively.

Test of Remaining Standards of Internal Control

The testing plan for the remaining four standards of internal control (Control Environment, Risk Assessment, Information and Communication, and Monitoring Activities) should include, at a minimum, the evaluation of each of the factors that were discussed in Section 3 – Planning Phase. Examples of testing procedures may include:

Control Environment

- Evaluate the "tone at the top" through inquiry, observation, focus groups, and surveys
- Obtain an understanding of, observe, and evaluate the process for handling exceptions to the agency's code of conduct
- Review the documented authorization levels and assess their reasonableness compared to the positions and responsibilities of the individuals
- Examine job descriptions for key financial reporting positions and evaluate whether employee understanding of roles and responsibilities is consistent with the description

Risk Assessment

- Review management's process for evaluating risks, including assessing the likelihood of occurrence and determining needed actions
- Evaluate whether management adequately addresses how it will identify and analyze significant estimates recorded in the financial statements

Information and Communication

- Evaluate senior management's involvement in the development of the strategic plan for information systems, including appropriate allocation of resources
- Obtain an understanding of the process for updating the accounting policy manual for new pronouncements and how updates are distributed to the appropriate individuals
- Inquire about the extent to which outside parties have been made aware of the agency's ethical standards and observe the process for addressing complaints from outside parties

Monitoring

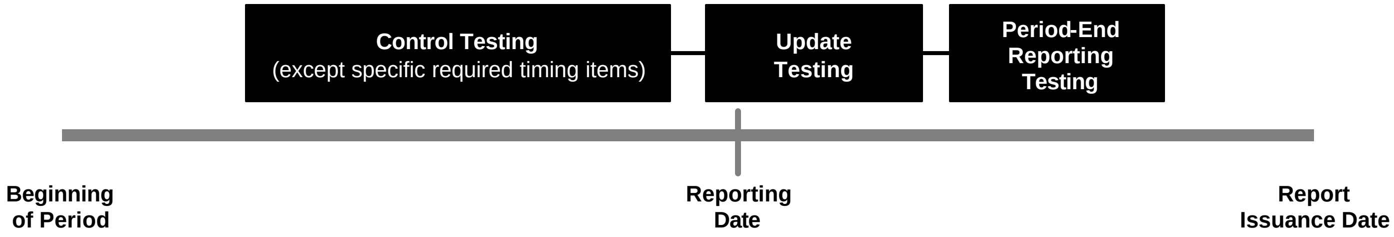
- Obtain an understanding of the monthly financial statement analysis process and observe how significant or unusual items are investigated and resolved
- Evaluate the effectiveness of the OIG and the process for reporting and following-up on identified internal control deficiencies
- Additionally, management must test its anti-fraud programs, and the effectiveness of the organization's Internal Control Committee.

Tests of these four Components of internal control will typically consist of inquiry, observation, and/or examination. Sufficient evidence should be obtained that these control Components are operating as designed. The sample sizes in the aforementioned table may not be appropriate due to the nature of controls being tested. In some cases, documentary evidence of controls or their performance does not exist and is not expected to exist. In these cases, management would make inquiries and observation of activities to support the controls that are in place[43].

Timing of Procedures

The time period over which an organization tests its internal control must be sufficient to determine operating effectiveness as of the end of the fiscal year. It would be unwise and impractical for the assessment team to perform all testing as of the end of the fiscal year, and it would not allow management sufficient time to remediate deficiencies. The following illustration depicts the potential period over which management should conduct its testing.

Figure 23: Time Period for Testing



Testing performed earlier in the year generally provides less evidence of effectiveness at the reporting date than testing performed later in the year and will require more extensive updating near year-end. For controls that cover (1) significant non-routine transactions, or (2) accounts or classes of transactions for which measurement involves a high degree of subjectivity or judgment, the assessment team should perform testing closer to or as of the reporting date rather than at an interim date. The assessment team's testing will invariably

[43] PCAOB AS 2.

uncover deficiencies that require remediation. The assessment team should take this into account when developing the project plan by estimating that a certain percentage of controls will have to be remediated and re-tested. The timing of testing should allow sufficient time for any necessary remediation efforts.

The assessment team's testing also encompasses controls that are relevant to the entity's financial reporting, even though such controls may not operate until after the entity's fiscal year-end. For example, some controls over the year-end closing process normally operate only after the reporting date. Accordingly, the assessment team's evaluation of the operating effectiveness of such controls occurs at the time that the controls are operating. Because testing these controls only in the year-end reporting process would not allow time to remediate any weaknesses.

Decisions about updating should be based on the significance of the specific controls, the testing results, and the length of the remaining period after interim testing. Update procedures could include a combination of:

- Inquiries of personnel to verify that the controls tested during the interim period are still in place (this type of testing alone would not be sufficient);
- Observation of the control being performed;
- Additional walkthroughs (i.e., inquiry and observation of one transaction through the process); and
- Testing of additional samples for more important and pervasive controls.

In situations where there have been significant changes in internal control during the year (e.g., changes that address deficiencies detected during interim testing), the assessment team must assess the operating effectiveness of the new controls between the time they were implemented and year-end. This period must be sufficient to enable management to obtain adequate evidence of the controls' operating effectiveness. For example, if a new monthly manual control is implemented in the middle of the fiscal year's last month, management may not have sufficient opportunity to assess its operating effectiveness.

Point of Focus 13

Timing of Testing

Various techniques are available to spread testing across the fiscal year. One method is to assess the sample over several quarters. For example, to reach a desired sample quantity of 60, management could test 15 instances in each quarter. The advantage of this technique is that management can obtain more frequent feedback on whether the control is working for purposes of the organization's quarterly reporting requirements.

Testing General Computer Controls

In virtually all entities, many of the controls that management relies on are automated or depend significantly on information systems and technology. As a result, management must evaluate the effectiveness of IT general controls to ensure the continuous, effective operation of the automated/information technology dependent controls. Given the technical skills necessary to evaluate general computer controls, management must determine whether the organization has personnel with the necessary expertise to perform this work or whether it must engage a specialist. When testing general computer controls, management must also consider the impact of implementing new accounting systems and the potential need to evaluate the new and old systems.

When evaluating and testing general computer controls, management should consider how each of the following FISCAM Domains and Critical Elements relate to internal control over financial reporting. (Note: The IT control environment should be assessed in a manner similar to the overall control environment)

Entity-wide Security Program Planning and Management (SP), FISCAM Section 3.1

Domain Objective: A framework and continuing cycle of activity exists for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the computer-related controls.

Management should document, test, and evaluate the controls in place to ensure that the following FISCAM Critical Element (control) objectives are addressed:

- Periodically assess risks
- Document an entity-wide security program plan
- Establish a security management structure and clearly assign security responsibilities
- Implement effective security-related personnel policies
- Monitor the security program's effectiveness and make changes as needed

Access Control (AC), FISCAM Section 3.2

Domain Objective: Access to system resources (e.g., programs, data, tables, and parameters) is restricted to properly authorized individuals for applications, databases, operating systems, and networks.

Management should document, test, and evaluate the controls in place to ensure that the following FISCAM Critical Element (control) objectives are addressed:

- Classify information resources according to their criticality and sensitivity
- Maintain a current list of authorized users and their access authorized
- Establish physical and logical controls to prevent or detect unauthorized access
- Monitor access, investigate apparent security violations, and take appropriate remedial action

Application Software Development and Change Control (CC), FISCAM Section 3.3

Domain Objective: New system and application development as well as existing system and application changes are authorized, tested, approved, properly implemented, and documented.

Management should document, test, and evaluate the controls in place to ensure that the following FISCAM Critical Element (control) objectives are addressed:

- Processing features and program modifications are properly authorized
- Test and approve all new and revised software
- Control software libraries

System Software (SS), FISCAM Section 3.4

Domain Objective: Access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system is limited and monitored.

Management should document, test, and evaluate the controls in place to ensure that the following FISCAM Critical Element (control) objectives are addressed:

- Limit access to system software
- Monitor access to and use of system software
- Control system software changes

Segregation of Duties (SD), FISCAM Section 3.5

Domain Objective: One individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

Management should document, test, and evaluate the controls in place to ensure that the following FISCAM Critical Element (control) objectives are addressed:

- Segregate incompatible duties and establish related policies
- Establish access controls to enforce segregation of duties
- Control personnel activities through formal operating procedures and supervision and review

Service Continuity (SC), FISCAM Section 3.6

Domain Objective: When unexpected events occur (i.e., disaster, service interruption, or loss of data), critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Management should document, test, and evaluate the controls in place to ensure that the following FISCAM Critical Element (control) objectives are addressed:

- Assess the criticality and sensitivity of computerized operations and identify supporting resources
- Take steps to prevent and minimize potential damage and interruption
- Develop and document a comprehensive contingency plan
- Periodically test the contingency plan and adjust it as appropriate

5.5 – Step 5: Document Test Results

Once the assessment team concludes test of controls it must document the results. The documentation will provide the support for management’s assertions; therefore, it will be reviewed by the independent public accountant and possibly by the GAO or OMB. Thus, the testing should be sufficiently documented to allow an independent person to understand and reperform the test, including the identification of the items tested (for example, the title and date of the report, invoice numbers, check numbers), who performed the testing, the test results, and the overall conclusion. When samples are used the following must be documented[44]:

- The sampling method used and any key factors regarding selection
- The sample size and the method of determining it
- The test procedures performed
- The results of tests, including evaluations of sample results
- Findings and conclusions

5.6 – Step 6: Evaluate the Test Results

The objective of evaluating test results is to conclude whether the controls are **operating effectively** to support the financial statement assertions**.** For example, consider the review and sign-off of a reconciliation of a subsidiary ledger to the general ledger. The assessment team must conclude, on the basis of the testing performed, whether the control effectively supports the completeness assertion. Other controls in the process would be tested to ensure that all transactions have been posted in the subsidiary ledger to support further the completeness assertion. And, still other controls would be tested to support the other relevant assertions such as valuation, existence and occurrence, rights and obligations, and presentation and disclosure. When evaluating the results and related evidence of specific tests, the following questions may be useful for consideration:

- What risk is the control intended to mitigate?
- Were exceptions found?
- Were exceptions resolved?
- Is there a process for correcting recurring exceptions?

In general, controls are tested on an accept/reject basis (i.e., a control is either working reliably or it is not). Also, a high level of assurance that controls are working effectively is required. To attain a high level of assurance regarding the operating effectiveness of a control, no more than a negligible exception rate can be accepted.

If an exception occurs in testing, the assessment team must evaluate the exception to determine why it occurred. Upon investigation of the exception, the assessment team may determine that the control is not operating effectively. Alternatively, the results of the investigation may not be conclusive that a deficiency exists. In this circumstance, assuming the control operates at least daily, the assessment team may select and test another sample of equal size. If no exceptions exist in the second sample, a conclusion that the overall exception rate is no more than negligible would typically be appropriate. In this case, the exception would not be considered a deficiency as the likelihood of misstatement is not more than remote. When an exception occurs in a quarterly, monthly, or weekly control, there is a strong indication that a deficiency exists due to the small populations involved (i.e., four quarters, 12 months, or 52 weeks). Additionally, the existence of compensating controls does not effect whether an internal control deficiency exists.

The assessment team should develop an inventory of all internal control deficiencies, significant deficiencies, and material weaknesses. The root cause for each deficiency should be documented and an assessment of

[44] Required sampling documentation adapted from the GAO/PCIE Financial Audit Manual, section 490

the necessary corrective action made (e.g., redesign the control or retrain the individuals involved)[45]. The assessment team should carefully assess each deficiency and prioritize remedial actions. Each remediated control will need to be retested to verify operating effectiveness.

Evidence of Remediated Control

The necessary length of time a control must be operating will depend on the frequency of the control's operation. The more often a control is performed, the shorter the time management will need to gather sufficient evidence that the control is operating effectively, as illustrated by the table below.

Figure 24: Remediated Control

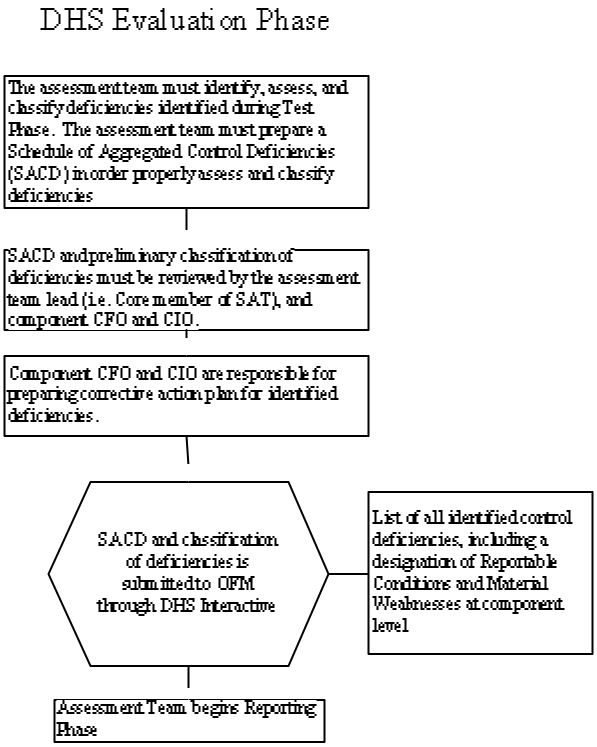
Frequency of Control	Suggested Time Period of Operation Prior to the Reporting Date
Quarterly	2 quarters*
Monthly	2 months
Weekly	5 weeks
Daily	20 days
Multiple Times per Day	25 times over a multiple day period

*Includes the fourth quarter as one of the quarters.

[45] OMB Circular A-123, pg 31

SECTION SIX: Evaluation Phase

Figure 25: Overview: The Evaluation Phase


DHS Evaluation Phase
The assessment team must identify, assess, and classify deficiencies identified during Test Phase. The assessment team must prepare a Schedule of Aggregated Control Deficiencies (SACD) in order properly assess and classify deficiencies
SACD and preliminary classification of deficiencies must be reviewed by the assessment team lead (i.e. Core member of SAT), and component CFO and CIO.
Component CFO and CIO are responsible for preparing corrective action plan for identified deficiencies.
SACD and classification of deficiencies is submitted to OFM through DHS Interactive
List of all identified control deficiencies, including a designation of Reportable Conditions and Material Weaknesses at component level
Assessment Team begins Reporting Phase

Purpose and Scope

Evaluating the significance of internal control deficiencies and reporting requires a significant degree of judgment.   The Evaluation Phase section describes the manner in which the assessment teams will, assess, and classify internal control deficiencies identified as a result of the testing of those controls.   Identification and assessment involve determining whether a deficiency is remote or inconsequential by assessing the magnitude and likelihood of misstatement.

Based on the assessment, deficiencies are classified as material weakness, reportable condition, or control deficiency. Once the assessment team has assessed and classified deficiencies identified during the testing phase. The assessment team must prepare a Schedule of Aggregated Control Deficiencies in order to properly assess and classify deficiencies. The SACD and preliminary classification of deficiencies must be reviewed by the assessment team lead and the Component CFO and CIO. Corrective actions plans must be prepared for by Component management under the supervision of the CFO and CIO. The SACD and final classification of deficiencies (i.e. Reportable Condition or Material Weaknesses) must be submitted to OFM through DHS interactive.

6.1 – Significance of Internal Control Deficiencies

Control deficiencies can range from control deficiencies to reportable conditions to material weaknesses in internal control. These are defined as follows[46]:

- **Control Deficiency -** Exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. Control deficiencies are internal to the organization and not reported externally.
- **Reportable Condition -** A control deficiency or combination of control deficiencies that adversely affects the Department's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with GAAP such that there is a more-than-remote[47] likelihood that a

[46] OMB Circular A-123, Section VI, page 18-19

[47] The term "remote" is defined in SFFAS No. 5, Accounting for Liabilities of the Federal Government, as the chance of the future event, or events, occurring is slight.

misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected. Reportable conditions are internal to the organization and not reported externally.

- A misstatement is **inconsequential** if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when combined with other misstatements, would **clearly be immaterial** to the financial statements or other significant reports. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement would be **more than inconsequential**.

- **Material Weakness -** A reportable condition, or combination of reportable conditions, that results in a more-than-remote[48] likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. Material weaknesses and a summary of corrective actions are reported through the PAR.

For all the above deficiencies, progress against corrective plans should be periodically assessed and reported to OFM by the Component Assessment Teams.

The following criteria can be used to assess the classification of an internal control deficiency, individually or in the aggregate, **after considering compensating controls**:

Figure 26: Classification of an Internal Control Deficiency

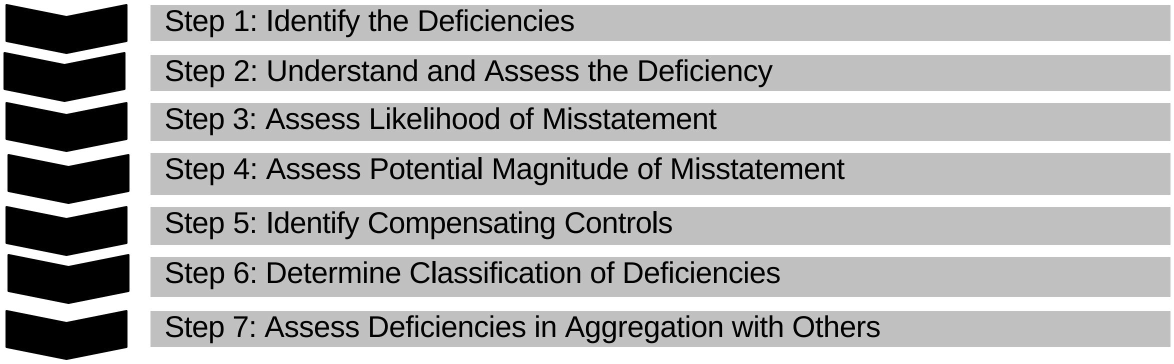
Classification of Deficiency	Likelihood of Misstatement		Potential Magnitude of Misstatement
Control Deficiency	Remote	OR	Inconsequential
Reportable Condition	More than remote	AND	More than inconsequential
Material Weakness	More than remote	AND	Material

6.2 – Identify, Assess, and Classify Internal Control Deficiencies

Identifying, assessing, and classifying internal control deficiencies requires a great deal of judgment. Deficiencies vary in type, likelihood, and magnitude. No simple model can adequately guide the assessment team through the process. Because of this, the guide presents the process in seven generalized steps to help the assessment team understand the concepts behind the process. Appendix S provides a detailed framework that the assessment team will use to assess and classify internal control deficiencies that are more than remote and more than inconsequential.

The seven steps for evaluating control deficiencies are as follows:

[48] Ibid



Step 1: Identify the Deficiencies

Step 2: Understand and Assess the Deficiency

Step 3: Assess Likelihood of Misstatement

Step 4: Assess Potential Magnitude of Misstatement

Step 5: Identify Compensating Controls

Step 6: Determine Classification of Deficiencies

Step 7: Assess Deficiencies in Aggregation with Others

6.2.1 – Step 1: Identify the Deficiencies

Internal control deficiencies may relate to the design or operating effectiveness of a control. The assessment team must consider deficiencies identified in all areas, including each of the five Components of internal control, entity-level controls, anti-fraud programs, etc. Deficiencies may be identified through many sources, including:

- Assessment team through its assessment of internal control over financial reporting
- Organization Management in a self-assessment process
- OIG in the scope of its work
- External Auditors in the scope of their work
- Service Organization SAS 70 reports
- GAO reports and other regulatory inspections

6.2.2 – Step 2: Understand and Assess the Deficiency

The assessment team should ensure that it has an accurate understanding of the nature and implications of the deficiency, as well as its potential impact on the financial statements or other significant financial reports. A focus on the financial statement assertion(s) that is not being supported as a result of the deficiency will assist in this understanding.

6.2.3 – Step 3: Assess Likelihood of Misstatement

The determination of likelihood is based on the potential that a misstatement would not be prevented or detected, not on whether a misstatement **has** occurred. Deficiencies for which there is only a remote likelihood of occurrence cannot rise to the level of a reportable condition or material weakness, and thus evaluation of the magnitude of a potential misstatement (Step 4) is not required.

The following factors may impact likelihood:

Figure 27: Assessing the Likelihood of Misstatement[49]

Likelihood
▪ The nature of the financial statement accounts, disclosures, and assertions involved;
▪ The susceptibility of the related assets or liability to loss or fraud (that is, greater susceptibility increases risk);
▪ The subjectivity, complexity, or extent of judgment required to determine the amount involved (that is greater subjectivity, complexity, or judgment, like that related to an accounting estimate, increases risk);
▪ The cause and frequency of known or detected exceptions for the operating effectiveness of a control;
▪ The interaction or relationship of the control with the other controls (that is, the interdependence or redundancy of the control);
▪ The interaction of the deficiencies; and
▪ The possible future consequences of the deficiency.

6.2.4 – Step 4 : Assess Potential Magnitude of Misstatement

Quantifying the impact of internal control deficiencies is difficult. The assessment team should consider the total account balance or transaction flow, and the assertion that is exposed to risk as a result of the deficiency. The focus should be on the size of the **potential** error that could occur in a more-than-remote likelihood situation. Accordingly, the assessment team must address whether the potential magnitude of the deficiency is more than inconsequential or material. The following factors may impact the magnitude:

Figure 28: Assessing the Potential Magnitude of Misstatement[50]

Magnitude
▪ The financial statement amounts or total of transactions exposed to the deficiency; and
▪ The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods.

6.2.5 – Step 5: Identify Compensating Controls

Control deficiencies should first be evaluated individually or in combination and then the determination of whether they are reportable conditions or material weaknesses should be made considering the effects of compensating controls. Compensating controls should be taken into account when assessing the likelihood of a misstatement occurring and not being prevented or detected. In addition, a compensating control may limit the potential magnitude of a deficiency (e.g., the compensating control only operates above a given dollar amount). However, the existence of a compensating control does not affect whether a control deficiency exists. If the Assessment team believes there are compensating controls in place that could address the financial statement assertion or risk resulting from the deficiency, it should consider and validate whether:

- The compensating control is effective; and

[49] PCAOB AS 2.

[50] Ibid.

- The compensating control would identify an error and address the assertion.

High-level analytical procedures are not sufficient to compensate for deficiencies. For a compensating control to be effective, the compensating control should operate at a level of precision that would prevent or detect a misstatement that was more than inconsequential or material, respectively. Additionally, if a misstatement occurred as the result of a deficiency, it is presumed that the compensating control, if it was effective, should have prevented or detected the misstatement.

6.2.6 – Step 6: Determine Classification of Deficiencies

Based on an assessment of the likelihood and magnitude of a misstatement resulting from an internal control deficiency, the assessment team should determine if the deficiency represents a control deficiency, reportable condition, or a material weakness. If the deficiency would prevent a prudent person from concluding that reasonable assurance exists that transactions are recorded to permit the preparation of the financial statements in conformity with GAAP, the deficiency should be at least a reportable condition. The detail guidance, in Appendix S, provides guidance about the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs. It also includes examples of internal control weaknesses that are ordinarily considered reportable conditions or possible material weaknesses.

Examples that illustrate when reportable conditions would become material weaknesses are included in Appendix M.

6.2.7 – Step 7: Assess Deficiencies in Aggregation with Others

As defined in Section 6.1, a reportable condition can be a combination of internal control deficiencies, and a material weakness can be a combination of reportable conditions. Thus, the assessment team must accumulate all internal control deficiencies for evaluation in the aggregate, considering whether there is a concentration of deficiencies over a particular process, account, or assertion. For example, assume a particular location has three internal control deficiencies in relation to accounts receivable processing. Although none of these deficiencies may individually be a reportable condition, they could potentially rise to this level when aggregated. The assessment of the interaction of deficiencies with each other is essentially a search for patterns (e.g., could the deficiencies affect the same financial statement accounts and assertions).

6.2.8 – Detail Framework for Evaluating Control Exceptions and Deficiencies[51]

The seven steps presented above provide a general understanding of the process used to evaluate deficiencies. If a deficiency is believed to be more than remote and more than inconsequential (reportable condition or material weakness), the assessment team should utilize the detail framework located in Appendix S to fully assess the likelihood and potential magnitude of misstatement.

6.3 – Remediation of Internal Control Deficiencies

Component Management is responsible for taking timely and effective action to correct deficiencies identified during the Testing Phase. Correcting deficiencies is an integral part of management accountability and must be considered a priority by the agency[52].

[51] Adapted from A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, 12/20/2004. The framework was created by the Big 4 and other Accounting Firms and accounting educators. The whitepaper was created based off of guidance available in AS2. The framework is based on the authors' views and is not intended to be applied universally and mechanically, but rather, with professional judgment.

[52] Adopted from OMB Circular A-123, Section V.

According to OMB Circular A-123, the extent to which corrective actions are tracked by management should be commensurate with the severity of the deficiency. Corrective action plans should be developed for all reportable conditions and material weaknesses, and progress against plans should be reported to OFM in a quarterly basis. For reportable conditions that are not included in the FMFIA report, CAPs should be developed and tracked internally at the appropriate level. A summary of the corrective action plans for material weaknesses should be included in the Department's PAR. The summary discussion should include a description of the material weakness, status of the corrective actions, and timeline for resolution[53].

Component management should maintain more detailed corrective action plans internally which should be available for OMB review. Component Management process for resolution and corrective action of identified material weaknesses in internal control must[54]:

- Provide for appointment of an overall corrective action accountability official from senior agency management. The corrective action accountability official should report to the agency's Senior Management Council;
- Require prompt resolution and corrective actions;
- Maintain accurate records of the status of the identified material weaknesses through the entire process of resolution and corrective action;
- Assure that the corrective action plans are consistent with laws, regulations and Departmental policy; and
- Assurance that performance appraisals of appropriate officials reflect effectiveness in resolving or implementing corrective action for identified material weaknesses[55].

A determination that a reportable condition has been corrected should be made only when sufficient corrective actions have been taken and the desired results achieved. This determination should be in writing, and along with other appropriate documentation supporting the determination, should be available for review by the OMB, the Senior Management Council, the OIG, and the external auditor.

As the Assessment team considers IG and GAO audit reports in identifying and correcting internal control deficiencies, they must be mindful of the statutory requirements for audit follow-up included in the IG Act, as amended and OMB Circular A-50, Audit Follow-up. The Senior Assessment Team and other applicable management have a responsibility to complete action, in a timely manner, on audit recommendations on which agreement with the IG has been reached. The Senior Assessment Team must make a decision regarding IG audit recommendation within a six month period after issuance of the audit report and implement management's decision within one year to the extent practicable. Refer to Appendix N for a copy of the DHS CAP Form.

Each Component should establish systems to assure the prompt and proper resolution and implementation of corrective action on identified material weaknesses. These systems provide for a complete record of action taken on the material weaknesses identified. A Management Directive will be issued to guide reporting of

[53] Ibid.

[54] Ibid.

[55] Standards based upon OMB Circular A-50, Audit Follow-up.

corrective actions plans. The process will be robust and will adapt formats prescribed by the GAO Yellow Book, as follows[56]:

- Criteria: The assessment team should provide information so that the ICC board will be able to determine the required or desired state or what is expected from the program or operation. The criteria are easier to understand when stated fairly, explicitly, and completely, and the source of the criteria is identified.[57]

- Condition: The assessment team should provide evidence of what was found in the actual situation. Reporting the scope or extent of the condition allows the report user to gain an accurate perspective.

- Cause: The assessment team should provide persuasive evidence on the factor or factors responsible for the difference between condition and criteria. In reporting the cause, the evidence should provide a reasonable and convincing argument for why the stated cause is the key factor or factors contributing to the difference as opposed to other possible causes, such as poorly designed criteria or factors uncontrollable by program management.

- Effect: The assessment team should provide a clear, logical link to establish the impact of the difference between the condition and the criteria. Effect is easier to understand when it is stated clearly, concisely, and, if possible, in quantifiable terms. The significance of the reported effect can be demonstrated through credible evidence.

In addition, a joint committee of representatives from the Chief Financial Officers Council Financial Management Policies and Practices Subcommittee and the President's Council on Integrity and Efficiency Audit Committee are currently drafting guidance for OMB Circular A-123 that will include guidance for addressing corrective action plans.

Remediated deficiencies may still need to be reported in the PAR. To be excluded from the PAR, the remediated control must be in place for a reasonable length of time to establish that it is functioning as intended during the reporting period. The general timeframe is displayed in the following table:

[56] GAO Government Audit Standards (Yellow Book) page 85.

[57] Common sources for criteria include laws, regulations, policies, procedures, and best and standard practices. The Standards for Internal Control in the Federal Government, (GAO/AIMD-00-21.31) and Internal Control – Integrated Framework, published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) are two sources of established criteria that can be used to support management's judgments and conclusions about internal control. The related Internal Control Management and Evaluation Tool that is found in this document provides a systematic, organized, and structured approach to assessing internal control.

Figure 29: General Timeframe

Frequency of Control	Suggested Time Period of Operation Prior to the Reporting Date
Quarterly	2 quarters[58]
Monthly	2 months
Weekly	5 weeks
Daily	20 days
Multiple Times per Day	25 times over a multiple day period

Testing will invariably uncover deficiencies that require remediation. The assessment team should take this into account when developing the project plan by estimating that a certain percentage of controls will have to be remediated and re-tested.

[58] Must include the fourth quarter as one of the quarters

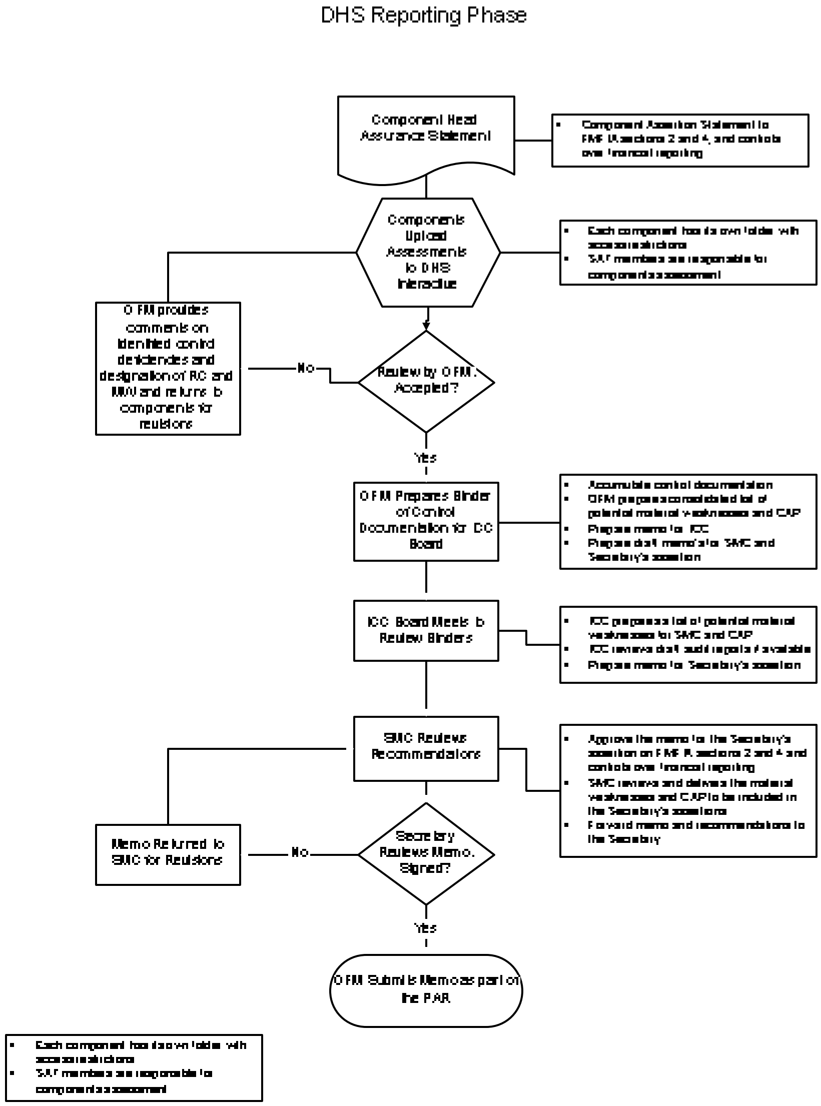
SECTION SEVEN: Reporting Phase

Purpose and Scope

This section describes procedures for reporting, including reporting requirements of the Components, ICC board, Senior Management Council, Secretary, and other matters related to reporting. The DHS Financial Accountability Act and OMB Circular A-123 require the DHS to report an annual assurance statement for internal control over financial reporting, material weaknesses, and the auditor's opinion externally in the PAR. The annual assurance statement for internal control over financial reporting is a subset of the overall Statement of Assurance and is based on the results of the internal control assessment process.

The following flowchart illustrates the DHS Internal Control Assessment reporting process:

Figure 30: Reporting Phase


DHS Reporting Phase
Component Head Assurance Statement
Component Assertion Statement to FMFIA sections 2 and 4, and controls over financial reporting
Components Upload Assessments to DHS Interactive
Each component has its own folder with access restrictions
SAT members are responsible for components assessment
OFM provides comments on identified control deficiencies and designation of RC and MW and returns to components for revisions
No
Review by OFM. Accepted?
Yes
OFM Prepares Binder of Control Documentation for ICC Board
Accumulate control documentation
OFM prepares consolidated list of potential material weaknesses and CAP
Prepare memo for ICC
Prepare draft memo's for SMC and Secretary's assertion
ICC Board Meets to Review Binders
ICC prepares list of potential material weaknesses for SMC and CAP
ICC reviews draft audit reports if available
Prepare memo for Secretary's assertion
SMC Reviews Recommendations
Approve the memo for the Secretary's assertion on FMFIA sections 2 and 4 and controls over financial reporting
SMC reviews and delivers the material weaknesses and CAP to be included in the Secretary's assertions
Forward memo and recommendations to the Secretary
Memo Returned to SMC for Revisions
No
Secretary Reviews Memo. Signed?
Yes
OFM Submits Memo as part of the PAR
Each component has its own folder with access restrictions
SAT members are responsible for components assessment

The following are the step for reporting on internal control over financial reporting:

Step 1: Required Reporting at the Component Level

Step 2: Required Reporting by OFM

Step 3: Required Reporting by ICC

Step 4: Required Reporting by SMC

Step 5: Required Reporting by DHS Secretary

7.1 – Step 1: Required Reporting at the Component Level

Each Component head is required to submit an annual Assurance Statement on FMFIA sections 2 and 4, and Internal Control over Financial Reporting. The assurance statements regarding internal control over financial reporting must be based on the results of the assessments conducted by their respective Component Assessment Team. The annual assurance statement must be submitted by the due date established by OFM via the Department's intranet site at https://interactive.dhs.gov. OFM will provide detailed guidance on submission procedures at a later date.

The assessment documentation (submitted to OFM during the documentation phase) accompanied by the organization head assurance statement will ultimately be reviewed by the Senior Management Council, and Internal Control Committee and will form the basis of the Secretary's Assessment of the Department's internal control over financial reporting.

7.2 – Step 2: Required Reporting by OFM

OFM will accumulate Component's assessment documentation and Component's assurance statements. Based on the Component's documentation, OFM will prepare a Department-wide consolidated list of material weaknesses along with a consolidated CAP (submitted by each Component quarterly and during the evaluation phase) for presentation to the ICC board. OFM will also prepare a draft Department-wide assurance statement on its preliminary assessment of internal control over financial reporting for ICC and Senior Management Council.

7.3 – Step 3: Required Reporting by ICC

At the establish date, the ICC board will meet to review assessment documentation along with OFM prepared consolidated list of material weaknesses, Department-wide CAP, and draft assurance statement. The ICC will make its own determination of material weaknesses and prepare a list of those that should be included in Secretary's assertion along with a Department-wide CAP. The ICC will then evaluate the OFM prepared assurance statement and make changes based on their assessment as necessary. The ICC prepared material weaknesses list along with the Department-wide CAP, and assurance statement will be submitted to the Senior Management Council for its consideration.

7.4 – Step 4: Required Reporting by SMC

The SMC will review the assurance statement, consolidated list of material weaknesses and Department-wide CAP prepared by the ICC. The SMC will review the documents and evaluate the conclusions made by the ICC. If the SMC agrees with the ICC conclusions, it will forward the assurance statement along with the reviewed consolidated list of material weaknesses and CAP to the Secretary for inclusion on the assertion.

7.5 – Step 5: Required Reporting by DHS Secretary

The Secretary will review the draft assurance statement, consolidated list of material weaknesses, and CAP. If approved, the assurance statement will be signed and provided to OFM for inclusion in the PAR.

7.6 – Content of Annual Statement of Assurance for Internal Control over Financial Reporting

This statement is management's assessment of the effectiveness of the agency's internal control over financial reporting as of September 30th of that fiscal year. Per OMB Circular A-123, this assurance statement is a subset of the overall Statement of Assurance required under Section 2 of the FMFIA and must include the following:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the agency;
- A statement identifying the OMB Circular A-123, Management's Responsibility for Internal Control as the framework used by the Senior Assessment Team to conduct the assessment of the effectiveness of the agency's internal control over financial reporting;
- An assessment of the effectiveness of the agency's internal control over financial reporting as of September 30, including an explicit conclusion as to whether the internal controls over financial reporting are effective; and
- All material weaknesses that exist as of September 30th of the current fiscal year.

According to OMB Circular A-123, in its assurance statement on the internal control over financial reporting, management is required to state a direct conclusion about whether the agency's internal control over financial reporting is effective. The statement must take one of the following forms:

- Unqualified statement of assurance (no material weaknesses reported);
- Qualified statement of assurance, considering the exceptions explicitly noted (one or more material weaknesses reported); or
- Statement of no assurance (no processes in place or pervasive material weaknesses).

Typically, the Senior Assessment Team is precluded from concluding that the agency's internal control over financial reporting is effective if there are one or more material weaknesses.

According to OMB Circular A-123, a summary of the CAPs for material weaknesses shall be included in the agency's PAR. The summary discussion shall include a description of the material weakness, status of corrective actions, and timeline for resolution[59].

7.7 – Required Communications

Communication between the Component Assessment Teams and the assessment team leads, CFO, CIO, and ICC board, is an important part of management's assessment. The assessment teams must communicate all reportable conditions and material weaknesses that it detects to the assessment team lead as they are identified. In turn the ICC board should communicate these findings to the auditor. These communications should be made at least quarterly. OFM will provide specific deadlines for this communication.

[59] OMB Circular A-123, pg 15

7.8 – Written Representations from Management to the Auditor for FY 2006

For management to receive an opinion on internal control over financial reporting, the auditor must receive the following representations from management[60]:

- Acknowledging management's responsibility for establishing and maintaining effective internal control over financial reporting;
- Stating that the Senior Assessment Team has performed an evaluation of the effectiveness of the entity's internal control over financial reporting and specifying the control criteria;
- Stating the Senior Assessment Team's assertion about the effectiveness of the entity's internal control over financial reporting is based on the control criteria as of a specified date;
- Stating that the Senior Assessment Team has disclosed to the auditor all deficiencies in the design or operation of internal control over financial that could adversely affect the entity's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements and has identified those that it believes to be reportable conditions or material weaknesses in internal control.
- Describing any material fraud and any other fraud that, although not material, involves senior management or management or other employees who have a significant role in the entity's internal control over financial reporting;
- Stating whether there were, subsequent to the date being reported on, any changes in internal control over financial reporting or other factors that might significantly affect internal control over financial reporting, including any corrective actions taken by the Senior Assessment Team with regard to reportable conditions and material weaknesses.

[60] Based on latest Draft of AT501 (February 2005) as found on the AICPA web site.

Appendix A – OMB Circular A-123 Appendix A Crosswalk to DHS Implementation Guide

The following crosswalk demonstrates how the Department's Implementation Guide complies with the requirements of OMB Circular A-123, Appendix A.

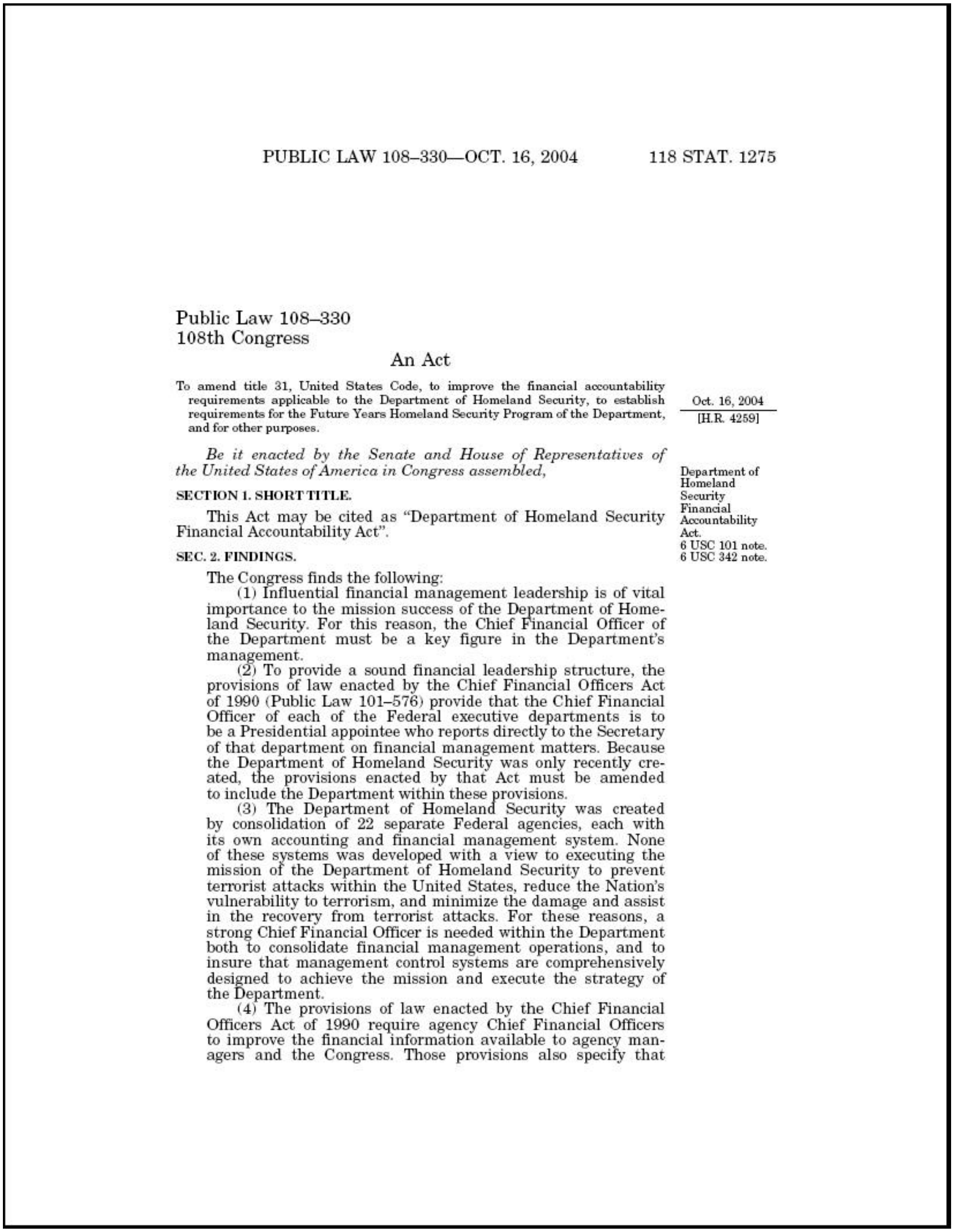
Figure 31: OMB Circular A-123 Appendix A Crosswalk to DHS Implementation Guide

OMB Circular A-123 Appendix A	DHS Implementation Guide
I. INTRODUCTION	**IMPLEMENTATION GUIDE**
I. Introduction	1.3 History of Internal Control in the Federal Government 1.5 Objectives of Internal Control over Financial Reporting and its Benefits
II. SCOPE	**IMPLEMENTATION GUIDE**
A. Objectives of Internal Control over Financial Reporting	1.5 Objectives of Internal Control over Financial Reporting and its Benefits
B. Definition of Financial Reporting	3.3 Identify Reports to be Included in the Assessment of 'Financial Reporting'
C. Planning Materiality	3.4 Identify Significant Line Items and related Accounts, Disclosures, and Processes/Cycles (including related transactions and systems)
D. Definition of Deficiencies	6.1 Significance of Internal Control Deficiencies
III. ASSESSING INTERNAL CONTROL OVER FINANCIAL REPORTING	**IMPLEMENTATION GUIDE**
A. Establish a Senior Assessment Team	1.6 Revision to OMB Circular A-123 and Appendix A 2.1 Project Oversight Appendix C – ICC Charter
B. Evaluate Internal Control at the Entity Level	See 1-5.
1. Control Environment	Appendix P – The Five Standards of Internal Control
2. Risk Assessment	Appendix P – The Five Standards of Internal Control
3. Control Activities	Appendix P – The Five Standards of Internal Control
4. Information and Communication	Appendix P – The Five Standards of Internal Control
5. Monitoring	Appendix P – The Five Standards of Internal Control
C. Evaluate Internal Control at the Process, Transaction, or Application Level	See 1-6.
1. Determine Significant Accounts or Groups of Accounts	3.4 Identify Significant Line Items and related Accounts, Disclosures, and Processes/Cycles (including related transactions and systems)
2. Identify and Evaluate the Major Classes of	3.4 Identify Significant Line Items and related

OMB Circular A-123 Appendix A	DHS Implementation Guide
Transactions	Accounts, Disclosures, and Processes/Cycles (including related transactions and systems)
3. Understand the Financial Reporting Process	3.4 Identify Significant Line Items and related Accounts, Disclosures, and Processes/Cycles (including related transactions and systems) 3.6.1 Period-End Reporting Process 4.2 Step 2: Prepare Walkthroughs
4. Gain an Understanding of Control Design to Achieve Management's Assertions	3.4 Identify Significant Line Items and related Accounts, Disclosures, and Processes/Cycles (including related transactions and systems) 4.2 Step 2: Prepare Walkthroughs
5. Controls Not Adequately Designed	4.4 Step 4: Assess the Design of Controls
6. Test Controls and Assess Compliance to Support Management's Assertions	5.4 Develop and Execute the Test Plans
D. Overall Assessment of the Design and Operation of Internal Control over Financial Reporting	4.4 Step 4: Assess the Design of Controls 5.6 Evaluate Test Results 6.2 Identify, Assess, and Classify Internal Control Deficiencies
E. Reliance on Other Work to Accomplish Assessment	3.7 Use of Service Organizations (ENTIRE 3.8.) 4.1.1 Use of Existing Documentation 5.2 Avoid duplication of efforts with other similar activities
IV. DOCUMENTATION	
A. Documenting Internal Control over Financial Reporting	4.1 Step 1: Determine Scope of Documentation 4.2 Step 2: Prepare Walkthroughs 4.1.1 Use of Existing Documentation 4.3 Step 3: Develop Control Documentation 7.1 Required Reporting at the Component Level 7.8 Written Representations from Management to the Auditor for FY 2006
B. Documenting the Assessment of Effectiveness	4.0 Documentation Phase
V. MANAGEMENT'S ASSURANCE STATEMENT ON INTERNAL CONTROL OVER FINANCIAL REPORTING	
V. Management's Assurance Statement on Internal Control over Financial Reporting	7.6 Content of Annual Assurance Statement of Assurance for Internal Control over Financial Reporting
A. Agencies Obtaining Audit Opinions on Internal Control	N/A due to the DHS Financial Accountability Act
VI. CORRECTING MATERIAL WEAKNESSESS IN INTERNAL CONTROL OVER FINANCIAL REPORTING	
VI. Correcting Material Weaknesses in Internal Control over Financial Reporting	6.3 Remediation of Internal Control Deficiencies
Exhibit 2: Sample Annual Assurance	

OMB Circular A-123 Appendix A	DHS Implementation Guide
Statement on Internal Control over Financial Reporting	
Sample Annual Assurance Statement	Not included.

Appendix B – Department of Homeland Security Financial Accountability Act



PUBLIC LAW 108–330—OCT. 16, 2004 118 STAT. 1275

Public Law 108–330
108th Congress

An Act

To amend title 31, United States Code, to improve the financial accountability requirements applicable to the Department of Homeland Security, to establish requirements for the Future Years Homeland Security Program of the Department, and for other purposes.

Oct. 16, 2004
[H.R. 4259]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Department of Homeland Security Financial Accountability Act.
6 USC 101 note.
6 USC 342 note.

SECTION 1. SHORT TITLE.

This Act may be cited as "Department of Homeland Security Financial Accountability Act".

SEC. 2. FINDINGS.

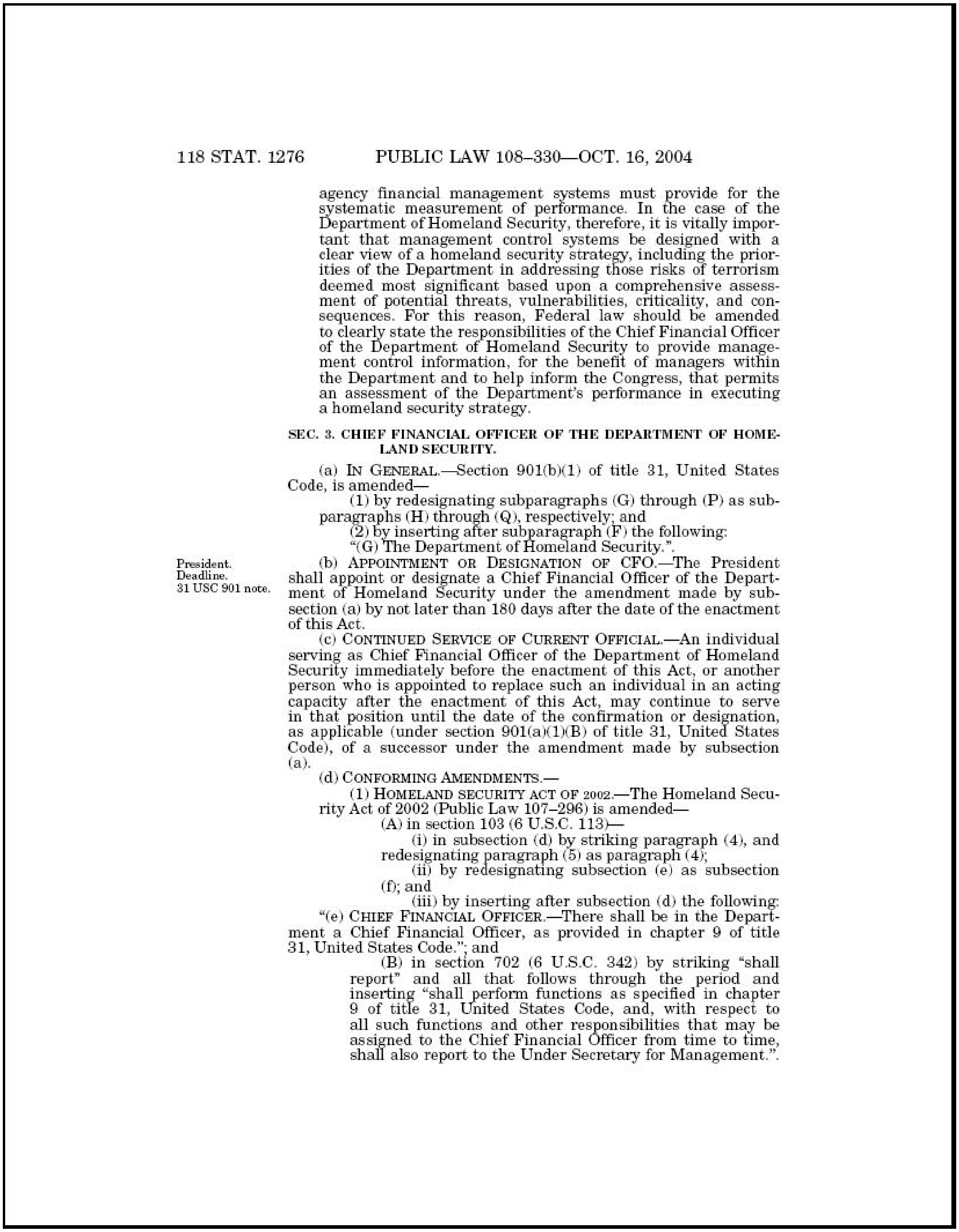
The Congress finds the following:

(1) Influential financial management leadership is of vital importance to the mission success of the Department of Homeland Security. For this reason, the Chief Financial Officer of the Department must be a key figure in the Department's management.

(2) To provide a sound financial leadership structure, the provisions of law enacted by the Chief Financial Officers Act of 1990 (Public Law 101–576) provide that the Chief Financial Officer of each of the Federal executive departments is to be a Presidential appointee who reports directly to the Secretary of that department on financial management matters. Because the Department of Homeland Security was only recently created, the provisions enacted by that Act must be amended to include the Department within these provisions.

(3) The Department of Homeland Security was created by consolidation of 22 separate Federal agencies, each with its own accounting and financial management system. None of these systems was developed with a view to executing the mission of the Department of Homeland Security to prevent terrorist attacks within the United States, reduce the Nation's vulnerability to terrorism, and minimize the damage and assist in the recovery from terrorist attacks. For these reasons, a strong Chief Financial Officer is needed within the Department both to consolidate financial management operations, and to insure that management control systems are comprehensively designed to achieve the mission and execute the strategy of the Department.

(4) The provisions of law enacted by the Chief Financial Officers Act of 1990 require agency Chief Financial Officers to improve the financial information available to agency managers and the Congress. Those provisions also specify that



118 STAT. 1276 PUBLIC LAW 108–330—OCT. 16, 2004

agency financial management systems must provide for the systematic measurement of performance. In the case of the Department of Homeland Security, therefore, it is vitally important that management control systems be designed with a clear view of a homeland security strategy, including the priorities of the Department in addressing those risks of terrorism deemed most significant based upon a comprehensive assessment of potential threats, vulnerabilities, criticality, and consequences. For this reason, Federal law should be amended to clearly state the responsibilities of the Chief Financial Officer of the Department of Homeland Security to provide management control information, for the benefit of managers within the Department and to help inform the Congress, that permits an assessment of the Department's performance in executing a homeland security strategy.

SEC. 3. CHIEF FINANCIAL OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 901(b)(1) of title 31, United States Code, is amended—

(1) by redesignating subparagraphs (G) through (P) as subparagraphs (H) through (Q), respectively; and

(2) by inserting after subparagraph (F) the following:

"(G) The Department of Homeland Security.".

President.
Deadline.
31 USC 901 note.

(b) APPOINTMENT OR DESIGNATION OF CFO.—The President shall appoint or designate a Chief Financial Officer of the Department of Homeland Security under the amendment made by subsection (a) by not later than 180 days after the date of the enactment of this Act.

(c) CONTINUED SERVICE OF CURRENT OFFICIAL.—An individual serving as Chief Financial Officer of the Department of Homeland Security immediately before the enactment of this Act, or another person who is appointed to replace such an individual in an acting capacity after the enactment of this Act, may continue to serve in that position until the date of the confirmation or designation, as applicable (under section 901(a)(1)(B) of title 31, United States Code), of a successor under the amendment made by subsection (a).

(d) CONFORMING AMENDMENTS.—

(1) HOMELAND SECURITY ACT OF 2002.—The Homeland Security Act of 2002 (Public Law 107–296) is amended—

(A) in section 103 (6 U.S.C. 113)—

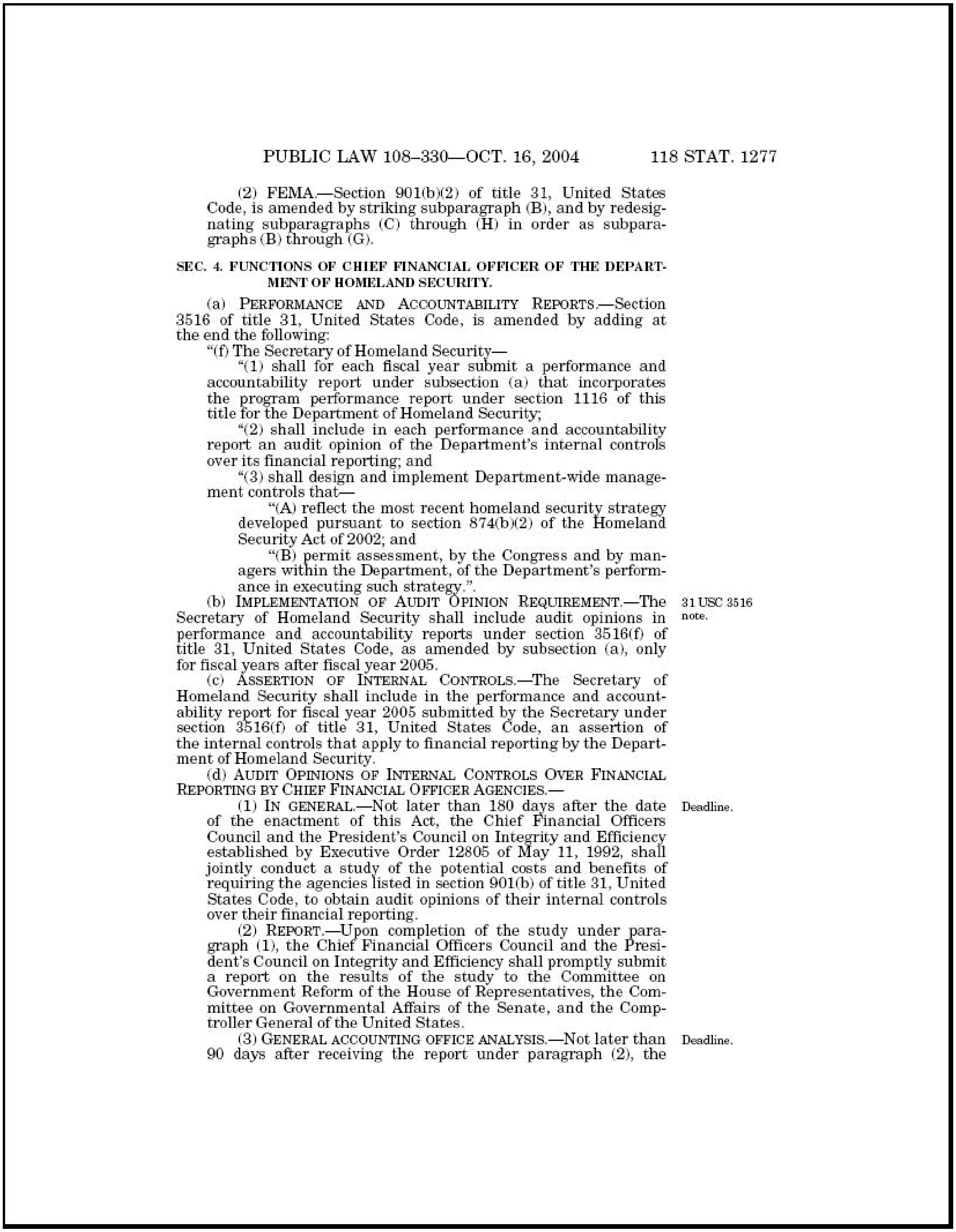
(i) in subsection (d) by striking paragraph (4), and redesignating paragraph (5) as paragraph (4);

(ii) by redesignating subsection (e) as subsection (f); and

(iii) by inserting after subsection (d) the following:

"(e) CHIEF FINANCIAL OFFICER.—There shall be in the Department a Chief Financial Officer, as provided in chapter 9 of title 31, United States Code."; and

(B) in section 702 (6 U.S.C. 342) by striking "shall report" and all that follows through the period and inserting "shall perform functions as specified in chapter 9 of title 31, United States Code, and, with respect to all such functions and other responsibilities that may be assigned to the Chief Financial Officer from time to time, shall also report to the Under Secretary for Management.".



PUBLIC LAW 108–330—OCT. 16, 2004 118 STAT. 1277

(2) FEMA.—Section 901(b)(2) of title 31, United States Code, is amended by striking subparagraph (B), and by redesignating subparagraphs (C) through (H) in order as subparagraphs (B) through (G).

SEC. 4. FUNCTIONS OF CHIEF FINANCIAL OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) PERFORMANCE AND ACCOUNTABILITY REPORTS.—Section 3516 of title 31, United States Code, is amended by adding at the end the following:

"(f) The Secretary of Homeland Security—

"(1) shall for each fiscal year submit a performance and accountability report under subsection (a) that incorporates the program performance report under section 1116 of this title for the Department of Homeland Security;

"(2) shall include in each performance and accountability report an audit opinion of the Department's internal controls over its financial reporting; and

"(3) shall design and implement Department-wide management controls that—

"(A) reflect the most recent homeland security strategy developed pursuant to section 874(b)(2) of the Homeland Security Act of 2002; and

"(B) permit assessment, by the Congress and by managers within the Department, of the Department's performance in executing such strategy.".

(b) IMPLEMENTATION OF AUDIT OPINION REQUIREMENT.—The Secretary of Homeland Security shall include audit opinions in performance and accountability reports under section 3516(f) of title 31, United States Code, as amended by subsection (a), only for fiscal years after fiscal year 2005. 31 USC 3516 note.

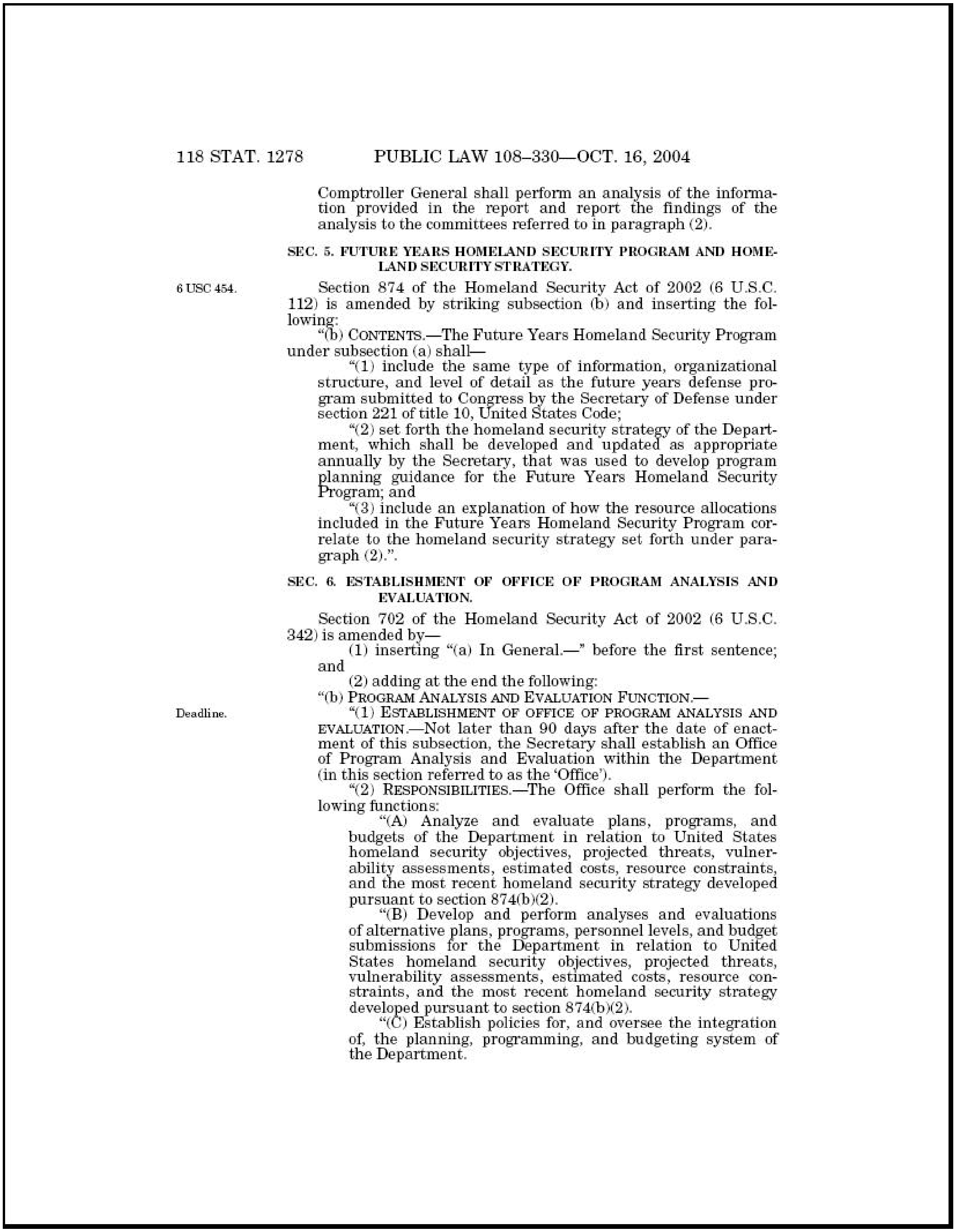
(c) ASSERTION OF INTERNAL CONTROLS.—The Secretary of Homeland Security shall include in the performance and accountability report for fiscal year 2005 submitted by the Secretary under section 3516(f) of title 31, United States Code, an assertion of the internal controls that apply to financial reporting by the Department of Homeland Security.

(d) AUDIT OPINIONS OF INTERNAL CONTROLS OVER FINANCIAL REPORTING BY CHIEF FINANCIAL OFFICER AGENCIES.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Chief Financial Officers Council and the President's Council on Integrity and Efficiency established by Executive Order 12805 of May 11, 1992, shall jointly conduct a study of the potential costs and benefits of requiring the agencies listed in section 901(b) of title 31, United States Code, to obtain audit opinions of their internal controls over their financial reporting. Deadline.

(2) REPORT.—Upon completion of the study under paragraph (1), the Chief Financial Officers Council and the President's Council on Integrity and Efficiency shall promptly submit a report on the results of the study to the Committee on Government Reform of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Comptroller General of the United States.

(3) GENERAL ACCOUNTING OFFICE ANALYSIS.—Not later than 90 days after receiving the report under paragraph (2), the Deadline.



Comptroller General shall perform an analysis of the information provided in the report and report the findings of the analysis to the committees referred to in paragraph (2).

SEC. 5. FUTURE YEARS HOMELAND SECURITY PROGRAM AND HOMELAND SECURITY STRATEGY.

6 USC 454. Section 874 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended by striking subsection (b) and inserting the following:

"(b) CONTENTS.—The Future Years Homeland Security Program under subsection (a) shall—

"(1) include the same type of information, organizational structure, and level of detail as the future years defense program submitted to Congress by the Secretary of Defense under section 221 of title 10, United States Code;

"(2) set forth the homeland security strategy of the Department, which shall be developed and updated as appropriate annually by the Secretary, that was used to develop program planning guidance for the Future Years Homeland Security Program; and

"(3) include an explanation of how the resource allocations included in the Future Years Homeland Security Program correlate to the homeland security strategy set forth under paragraph (2).".

SEC. 6. ESTABLISHMENT OF OFFICE OF PROGRAM ANALYSIS AND EVALUATION.

Section 702 of the Homeland Security Act of 2002 (6 U.S.C. 342) is amended by—

(1) inserting "(a) In General.—" before the first sentence; and

(2) adding at the end the following:

"(b) PROGRAM ANALYSIS AND EVALUATION FUNCTION.—

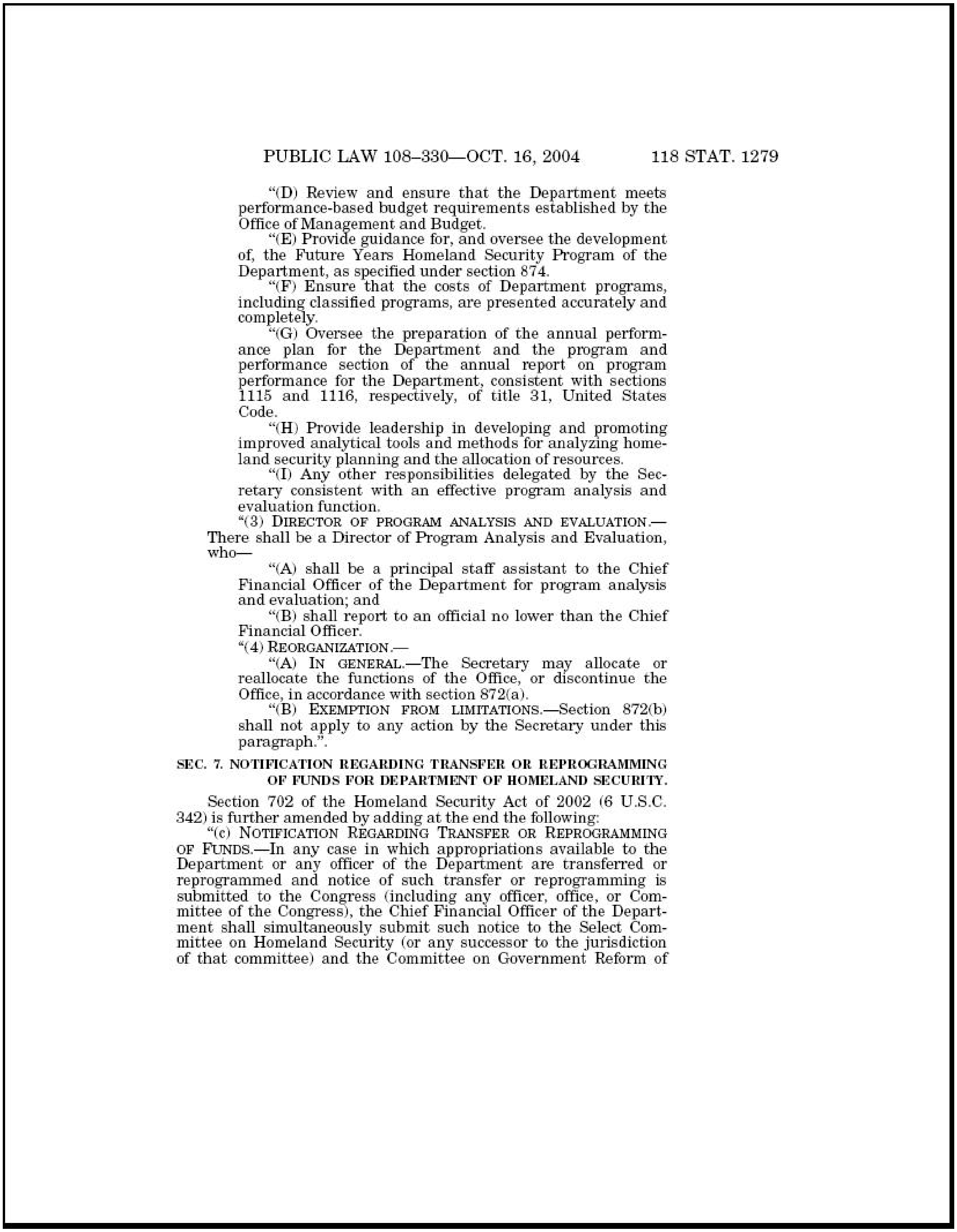
Deadline. "(1) ESTABLISHMENT OF OFFICE OF PROGRAM ANALYSIS AND EVALUATION.—Not later than 90 days after the date of enactment of this subsection, the Secretary shall establish an Office of Program Analysis and Evaluation within the Department (in this section referred to as the 'Office').

"(2) RESPONSIBILITIES.—The Office shall perform the following functions:

"(A) Analyze and evaluate plans, programs, and budgets of the Department in relation to United States homeland security objectives, projected threats, vulnerability assessments, estimated costs, resource constraints, and the most recent homeland security strategy developed pursuant to section 874(b)(2).

"(B) Develop and perform analyses and evaluations of alternative plans, programs, personnel levels, and budget submissions for the Department in relation to United States homeland security objectives, projected threats, vulnerability assessments, estimated costs, resource constraints, and the most recent homeland security strategy developed pursuant to section 874(b)(2).

"(C) Establish policies for, and oversee the integration of, the planning, programming, and budgeting system of the Department.



PUBLIC LAW 108–330—OCT. 16, 2004 118 STAT. 1279

“(D) Review and ensure that the Department meets performance-based budget requirements established by the Office of Management and Budget.

“(E) Provide guidance for, and oversee the development of, the Future Years Homeland Security Program of the Department, as specified under section 874.

“(F) Ensure that the costs of Department programs, including classified programs, are presented accurately and completely.

“(G) Oversee the preparation of the annual performance plan for the Department and the program and performance section of the annual report on program performance for the Department, consistent with sections 1115 and 1116, respectively, of title 31, United States Code.

“(H) Provide leadership in developing and promoting improved analytical tools and methods for analyzing homeland security planning and the allocation of resources.

“(I) Any other responsibilities delegated by the Secretary consistent with an effective program analysis and evaluation function.

“(3) Director of Program Analysis and Evaluation.—There shall be a Director of Program Analysis and Evaluation, who—

“(A) shall be a principal staff assistant to the Chief Financial Officer of the Department for program analysis and evaluation; and

“(B) shall report to an official no lower than the Chief Financial Officer.

“(4) Reorganization.—

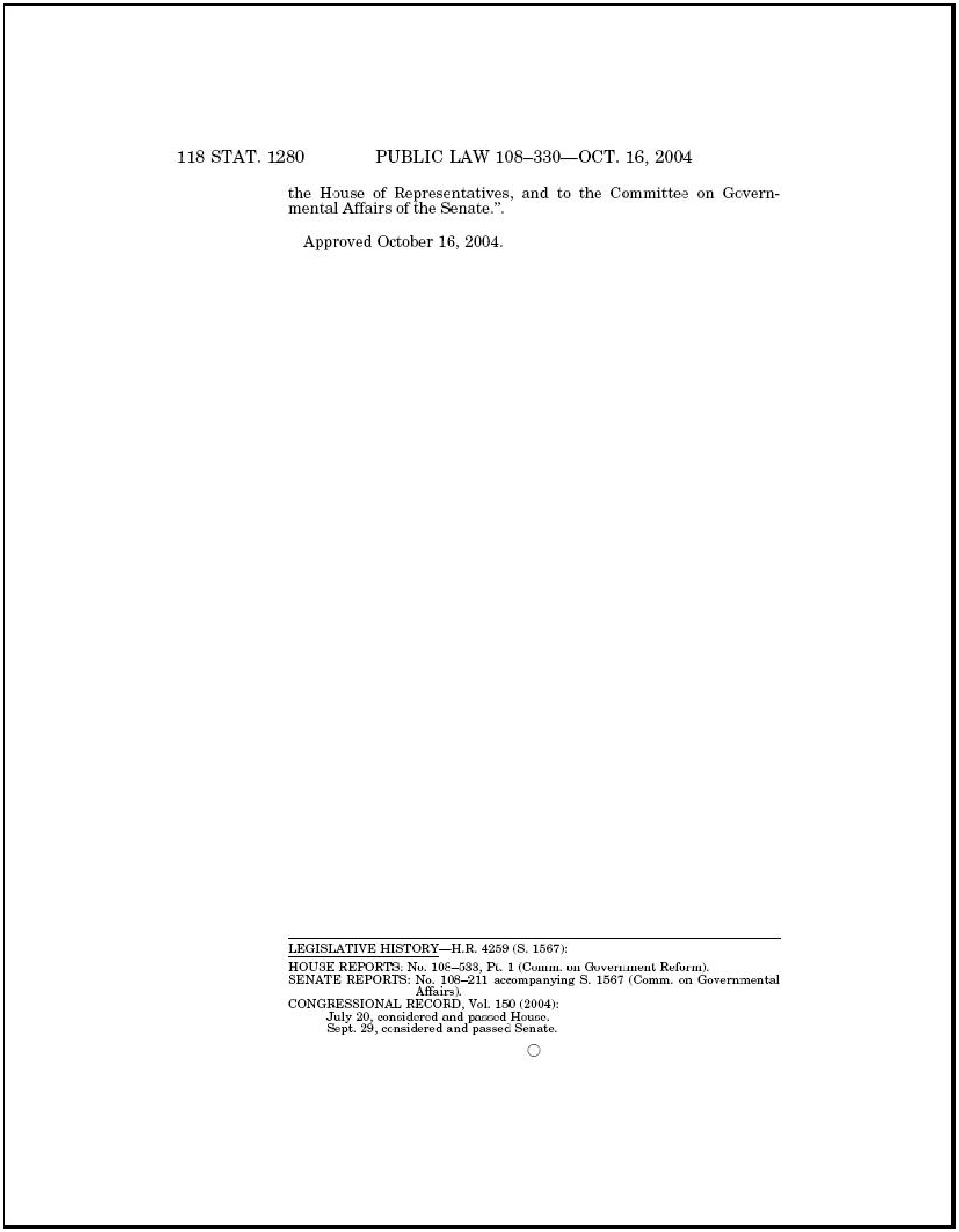
“(A) In general.—The Secretary may allocate or reallocate the functions of the Office, or discontinue the Office, in accordance with section 872(a).

“(B) Exemption from limitations.—Section 872(b) shall not apply to any action by the Secretary under this paragraph.”.

SEC. 7. NOTIFICATION REGARDING TRANSFER OR REPROGRAMMING OF FUNDS FOR DEPARTMENT OF HOMELAND SECURITY.

Section 702 of the Homeland Security Act of 2002 (6 U.S.C. 342) is further amended by adding at the end the following:

“(c) Notification Regarding Transfer or Reprogramming of Funds.—In any case in which appropriations available to the Department or any officer of the Department are transferred or reprogrammed and notice of such transfer or reprogramming is submitted to the Congress (including any officer, office, or Committee of the Congress), the Chief Financial Officer of the Department shall simultaneously submit such notice to the Select Committee on Homeland Security (or any successor to the jurisdiction of that committee) and the Committee on Government Reform of



118 STAT. 1280 PUBLIC LAW 108–330—OCT. 16, 2004

the House of Representatives, and to the Committee on Governmental Affairs of the Senate.”.

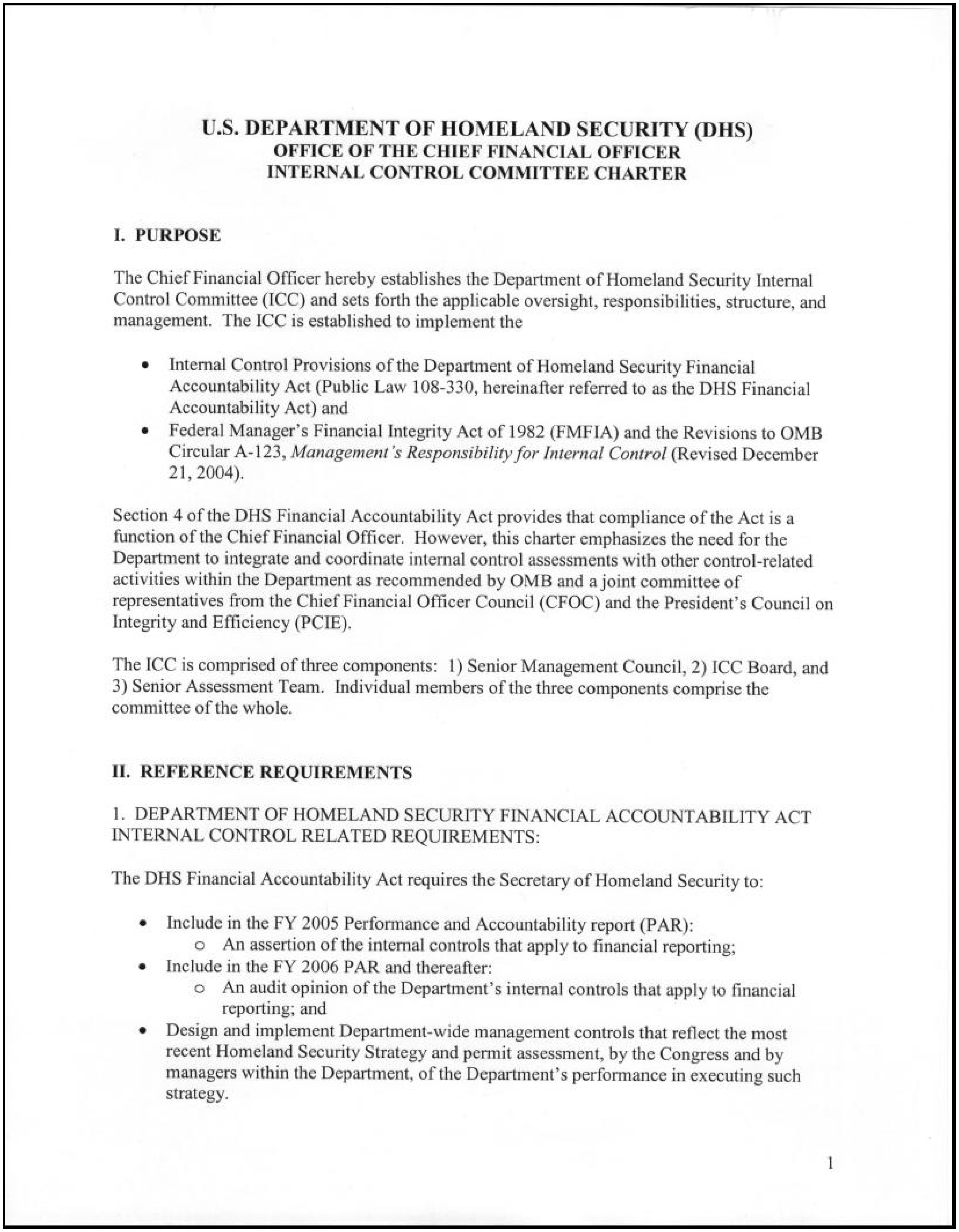
Approved October 16, 2004.

LEGISLATIVE HISTORY—H.R. 4259 (S. 1567):

HOUSE REPORTS: No. 108–533, Pt. 1 (Comm. on Government Reform).
SENATE REPORTS: No. 108–211 accompanying S. 1567 (Comm. on Governmental Affairs).
CONGRESSIONAL RECORD, Vol. 150 (2004):
July 20, considered and passed House.
Sept. 29, considered and passed Senate.

○

Appendix C – Internal Control Committee Charter



U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)
OFFICE OF THE CHIEF FINANCIAL OFFICER
INTERNAL CONTROL COMMITTEE CHARTER

I. PURPOSE

The Chief Financial Officer hereby establishes the Department of Homeland Security Internal Control Committee (ICC) and sets forth the applicable oversight, responsibilities, structure, and management. The ICC is established to implement the

- Internal Control Provisions of the Department of Homeland Security Financial Accountability Act (Public Law 108-330, hereinafter referred to as the DHS Financial Accountability Act) and
- Federal Manager's Financial Integrity Act of 1982 (FMFIA) and the Revisions to OMB Circular A-123, *Management's Responsibility for Internal Control* (Revised December 21, 2004).

Section 4 of the DHS Financial Accountability Act provides that compliance of the Act is a function of the Chief Financial Officer. However, this charter emphasizes the need for the Department to integrate and coordinate internal control assessments with other control-related activities within the Department as recommended by OMB and a joint committee of representatives from the Chief Financial Officer Council (CFOC) and the President's Council on Integrity and Efficiency (PCIE).

The ICC is comprised of three components: 1) Senior Management Council, 2) ICC Board, and 3) Senior Assessment Team. Individual members of the three components comprise the committee of the whole.

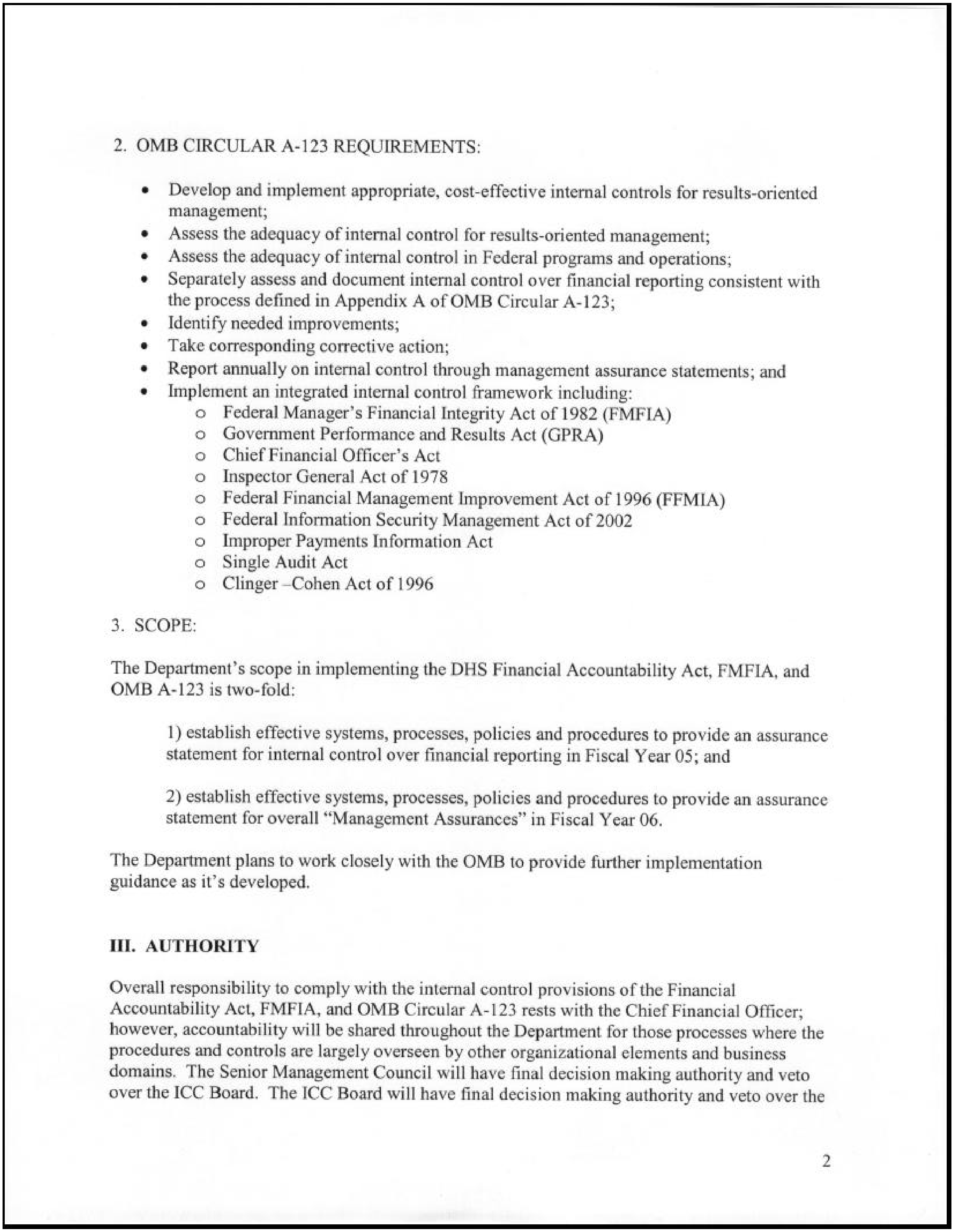
II. REFERENCE REQUIREMENTS

1. DEPARTMENT OF HOMELAND SECURITY FINANCIAL ACCOUNTABILITY ACT INTERNAL CONTROL RELATED REQUIREMENTS:

The DHS Financial Accountability Act requires the Secretary of Homeland Security to:

- Include in the FY 2005 Performance and Accountability report (PAR):
  - An assertion of the internal controls that apply to financial reporting;
- Include in the FY 2006 PAR and thereafter:
  - An audit opinion of the Department's internal controls that apply to financial reporting; and
- Design and implement Department-wide management controls that reflect the most recent Homeland Security Strategy and permit assessment, by the Congress and by managers within the Department, of the Department's performance in executing such strategy.

1



2. OMB CIRCULAR A-123 REQUIREMENTS:

- Develop and implement appropriate, cost-effective internal controls for results-oriented management;
- Assess the adequacy of internal control for results-oriented management;
- Assess the adequacy of internal control in Federal programs and operations;
- Separately assess and document internal control over financial reporting consistent with the process defined in Appendix A of OMB Circular A-123;
- Identify needed improvements;
- Take corresponding corrective action;
- Report annually on internal control through management assurance statements; and
- Implement an integrated internal control framework including:
    - Federal Manager's Financial Integrity Act of 1982 (FMFIA)
    - Government Performance and Results Act (GPRA)
    - Chief Financial Officer's Act
    - Inspector General Act of 1978
    - Federal Financial Management Improvement Act of 1996 (FFMIA)
    - Federal Information Security Management Act of 2002
    - Improper Payments Information Act
    - Single Audit Act
    - Clinger –Cohen Act of 1996

3. SCOPE:

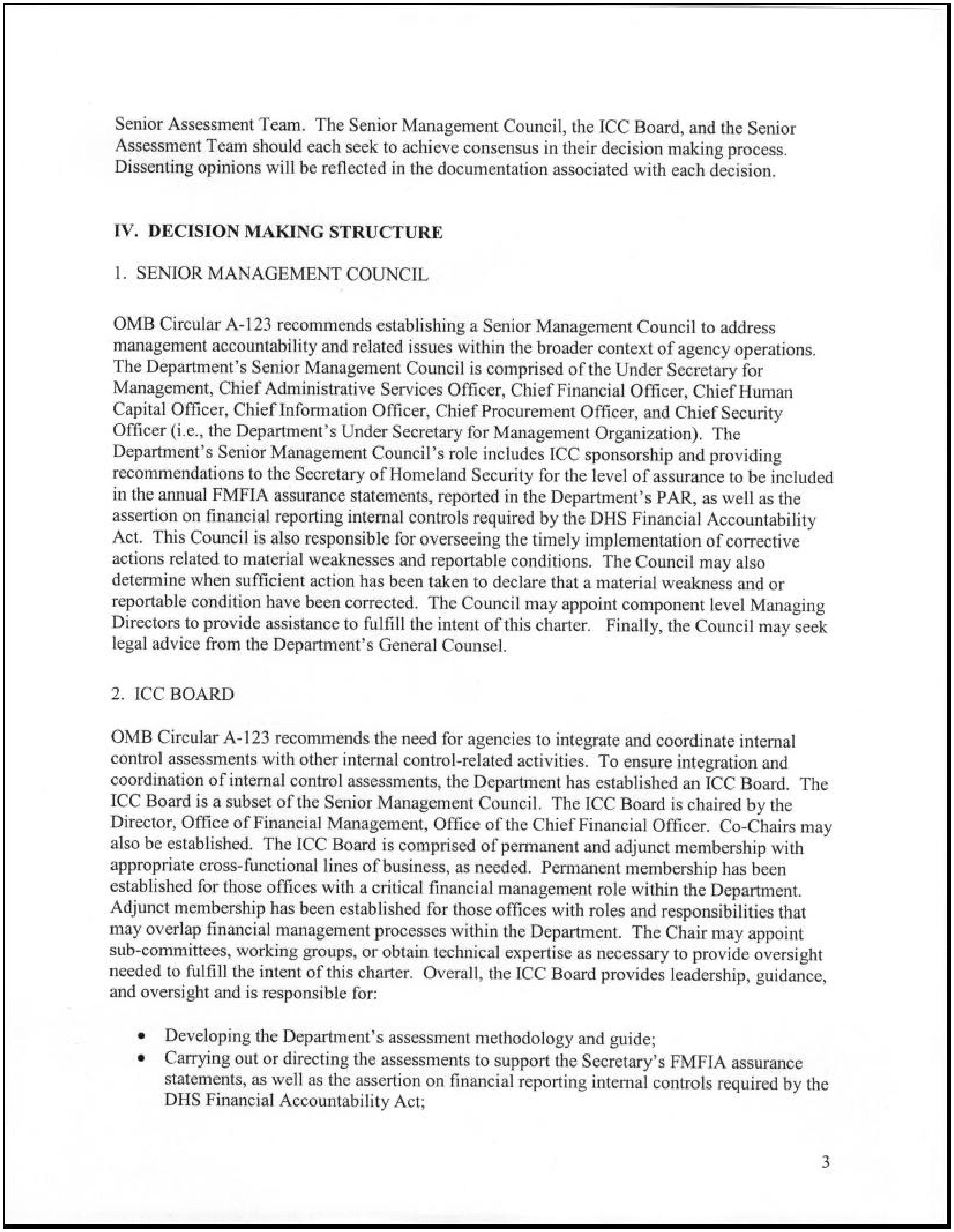
The Department's scope in implementing the DHS Financial Accountability Act, FMFIA, and OMB A-123 is two-fold:

> 1) establish effective systems, processes, policies and procedures to provide an assurance statement for internal control over financial reporting in Fiscal Year 05; and
>
> 2) establish effective systems, processes, policies and procedures to provide an assurance statement for overall "Management Assurances" in Fiscal Year 06.

The Department plans to work closely with the OMB to provide further implementation guidance as it's developed.

III. AUTHORITY

Overall responsibility to comply with the internal control provisions of the Financial Accountability Act, FMFIA, and OMB Circular A-123 rests with the Chief Financial Officer; however, accountability will be shared throughout the Department for those processes where the procedures and controls are largely overseen by other organizational elements and business domains. The Senior Management Council will have final decision making authority and veto over the ICC Board. The ICC Board will have final decision making authority and veto over the



Senior Assessment Team. The Senior Management Council, the ICC Board, and the Senior Assessment Team should each seek to achieve consensus in their decision making process. Dissenting opinions will be reflected in the documentation associated with each decision.

IV. DECISION MAKING STRUCTURE

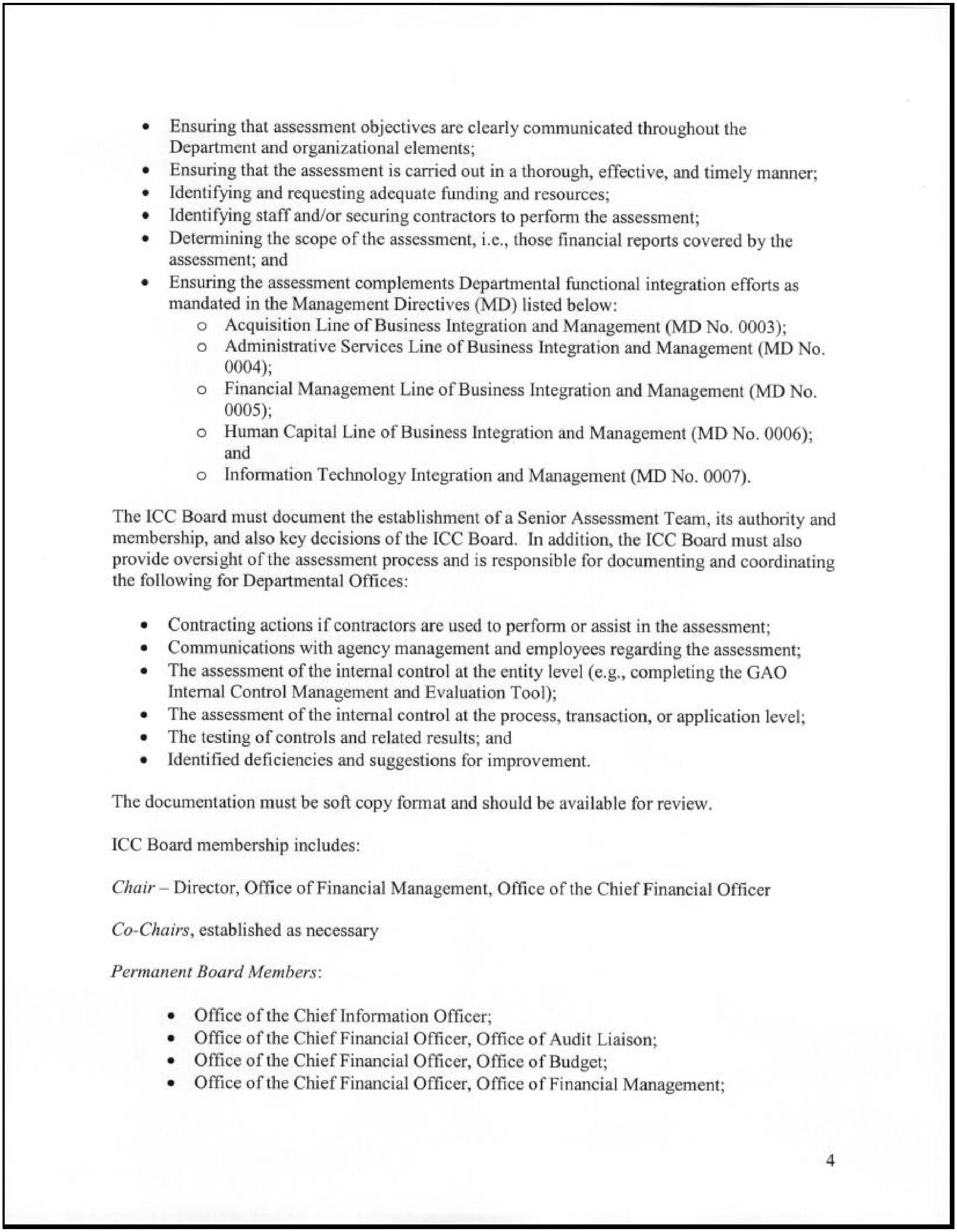
1. SENIOR MANAGEMENT COUNCIL

OMB Circular A-123 recommends establishing a Senior Management Council to address management accountability and related issues within the broader context of agency operations. The Department's Senior Management Council is comprised of the Under Secretary for Management, Chief Administrative Services Officer, Chief Financial Officer, Chief Human Capital Officer, Chief Information Officer, Chief Procurement Officer, and Chief Security Officer (i.e., the Department's Under Secretary for Management Organization). The Department's Senior Management Council's role includes ICC sponsorship and providing recommendations to the Secretary of Homeland Security for the level of assurance to be included in the annual FMFIA assurance statements, reported in the Department's PAR, as well as the assertion on financial reporting internal controls required by the DHS Financial Accountability Act. This Council is also responsible for overseeing the timely implementation of corrective actions related to material weaknesses and reportable conditions. The Council may also determine when sufficient action has been taken to declare that a material weakness and or reportable condition have been corrected. The Council may appoint component level Managing Directors to provide assistance to fulfill the intent of this charter. Finally, the Council may seek legal advice from the Department's General Counsel.

2. ICC BOARD

OMB Circular A-123 recommends the need for agencies to integrate and coordinate internal control assessments with other internal control-related activities. To ensure integration and coordination of internal control assessments, the Department has established an ICC Board. The ICC Board is a subset of the Senior Management Council. The ICC Board is chaired by the Director, Office of Financial Management, Office of the Chief Financial Officer. Co-Chairs may also be established. The ICC Board is comprised of permanent and adjunct membership with appropriate cross-functional lines of business, as needed. Permanent membership has been established for those offices with a critical financial management role within the Department. Adjunct membership has been established for those offices with roles and responsibilities that may overlap financial management processes within the Department. The Chair may appoint sub-committees, working groups, or obtain technical expertise as necessary to provide oversight needed to fulfill the intent of this charter. Overall, the ICC Board provides leadership, guidance, and oversight and is responsible for:

- Developing the Department's assessment methodology and guide;
- Carrying out or directing the assessments to support the Secretary's FMFIA assurance statements, as well as the assertion on financial reporting internal controls required by the DHS Financial Accountability Act;



- Ensuring that assessment objectives are clearly communicated throughout the Department and organizational elements;
- Ensuring that the assessment is carried out in a thorough, effective, and timely manner;
- Identifying and requesting adequate funding and resources;
- Identifying staff and/or securing contractors to perform the assessment;
- Determining the scope of the assessment, i.e., those financial reports covered by the assessment; and
- Ensuring the assessment complements Departmental functional integration efforts as mandated in the Management Directives (MD) listed below:
    - Acquisition Line of Business Integration and Management (MD No. 0003);
    - Administrative Services Line of Business Integration and Management (MD No. 0004);
    - Financial Management Line of Business Integration and Management (MD No. 0005);
    - Human Capital Line of Business Integration and Management (MD No. 0006); and
    - Information Technology Integration and Management (MD No. 0007).

The ICC Board must document the establishment of a Senior Assessment Team, its authority and membership, and also key decisions of the ICC Board. In addition, the ICC Board must also provide oversight of the assessment process and is responsible for documenting and coordinating the following for Departmental Offices:

- Contracting actions if contractors are used to perform or assist in the assessment;
- Communications with agency management and employees regarding the assessment;
- The assessment of the internal control at the entity level (e.g., completing the GAO Internal Control Management and Evaluation Tool);
- The assessment of the internal control at the process, transaction, or application level;
- The testing of controls and related results; and
- Identified deficiencies and suggestions for improvement.

The documentation must be soft copy format and should be available for review.

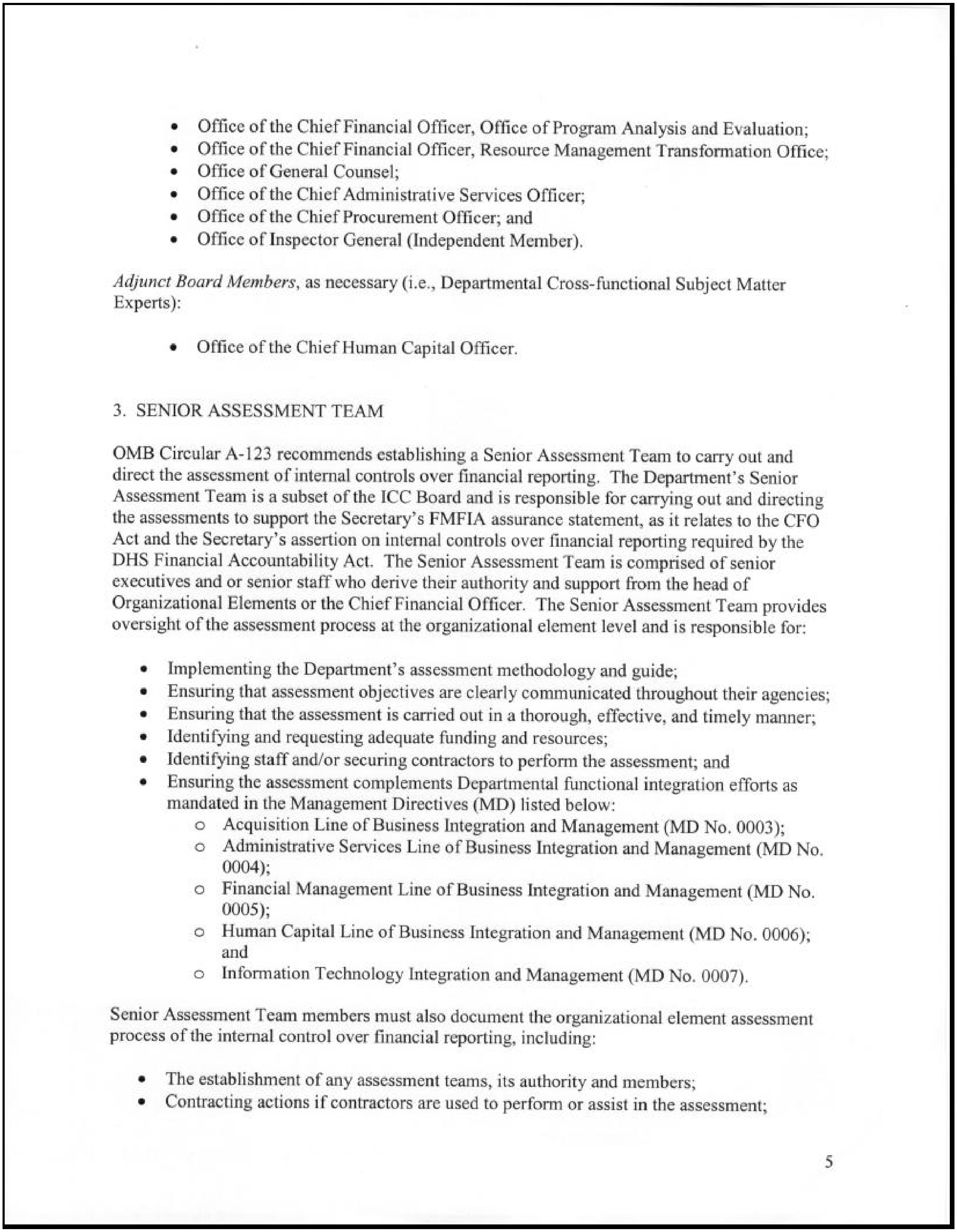
ICC Board membership includes:

Chair – Director, Office of Financial Management, Office of the Chief Financial Officer

Co-Chairs, established as necessary

Permanent Board Members:

- Office of the Chief Information Officer;
- Office of the Chief Financial Officer, Office of Audit Liaison;
- Office of the Chief Financial Officer, Office of Budget;
- Office of the Chief Financial Officer, Office of Financial Management;



- Office of the Chief Financial Officer, Office of Program Analysis and Evaluation;
- Office of the Chief Financial Officer, Resource Management Transformation Office;
- Office of General Counsel;
- Office of the Chief Administrative Services Officer;
- Office of the Chief Procurement Officer; and
- Office of Inspector General (Independent Member).

Adjunct Board Members, as necessary (i.e., Departmental Cross-functional Subject Matter Experts):

- Office of the Chief Human Capital Officer.

3. SENIOR ASSESSMENT TEAM

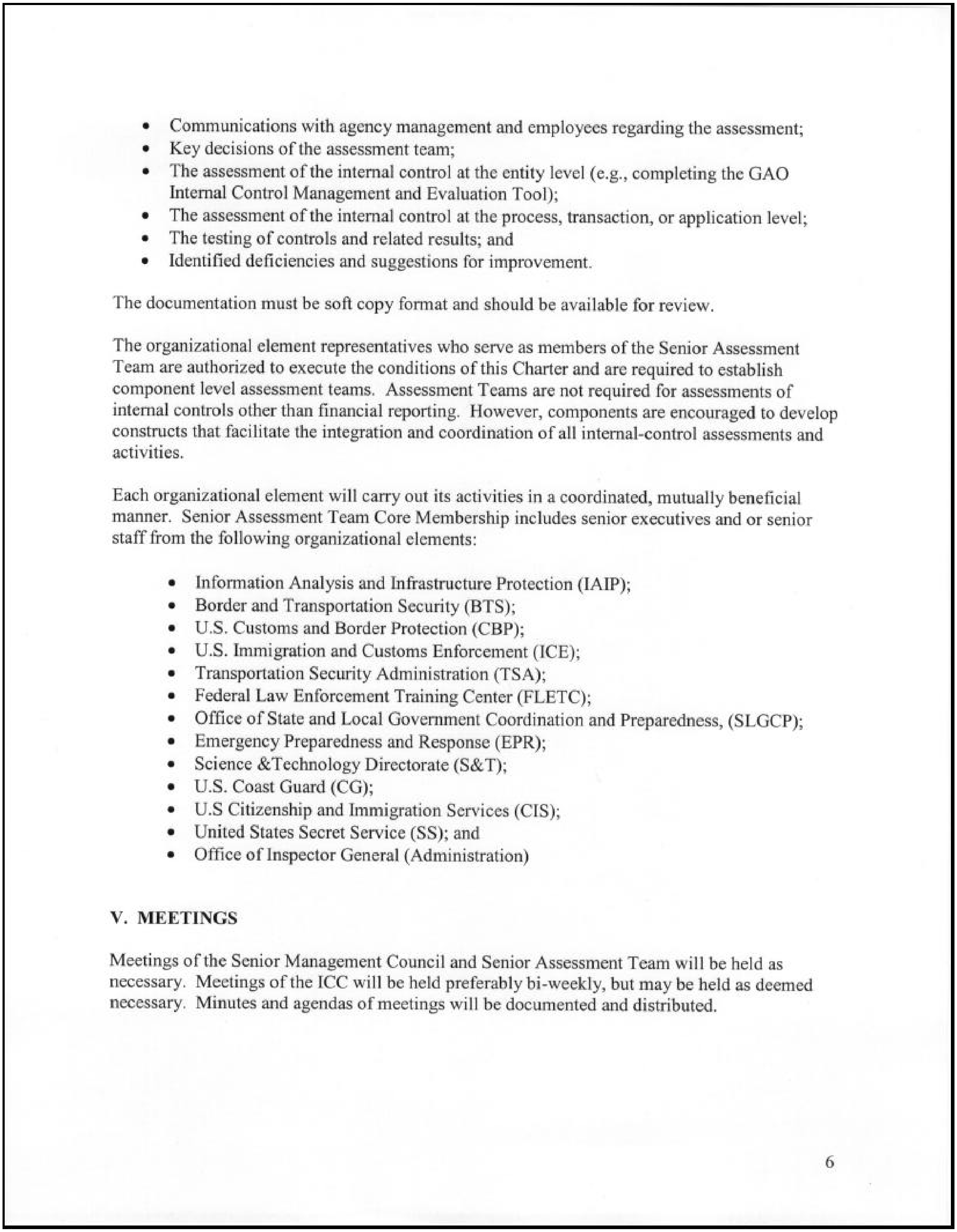
OMB Circular A-123 recommends establishing a Senior Assessment Team to carry out and direct the assessment of internal controls over financial reporting. The Department's Senior Assessment Team is a subset of the ICC Board and is responsible for carrying out and directing the assessments to support the Secretary's FMFIA assurance statement, as it relates to the CFO Act and the Secretary's assertion on internal controls over financial reporting required by the DHS Financial Accountability Act. The Senior Assessment Team is comprised of senior executives and or senior staff who derive their authority and support from the head of Organizational Elements or the Chief Financial Officer. The Senior Assessment Team provides oversight of the assessment process at the organizational element level and is responsible for:

- Implementing the Department's assessment methodology and guide;
- Ensuring that assessment objectives are clearly communicated throughout their agencies;
- Ensuring that the assessment is carried out in a thorough, effective, and timely manner;
- Identifying and requesting adequate funding and resources;
- Identifying staff and/or securing contractors to perform the assessment; and
- Ensuring the assessment complements Departmental functional integration efforts as mandated in the Management Directives (MD) listed below:
  - Acquisition Line of Business Integration and Management (MD No. 0003);
  - Administrative Services Line of Business Integration and Management (MD No. 0004);
  - Financial Management Line of Business Integration and Management (MD No. 0005);
  - Human Capital Line of Business Integration and Management (MD No. 0006); and
  - Information Technology Integration and Management (MD No. 0007).

Senior Assessment Team members must also document the organizational element assessment process of the internal control over financial reporting, including:

- The establishment of any assessment teams, its authority and members;
- Contracting actions if contractors are used to perform or assist in the assessment;

5



- Communications with agency management and employees regarding the assessment;
- Key decisions of the assessment team;
- The assessment of the internal control at the entity level (e.g., completing the GAO Internal Control Management and Evaluation Tool);
- The assessment of the internal control at the process, transaction, or application level;
- The testing of controls and related results; and
- Identified deficiencies and suggestions for improvement.

The documentation must be soft copy format and should be available for review.

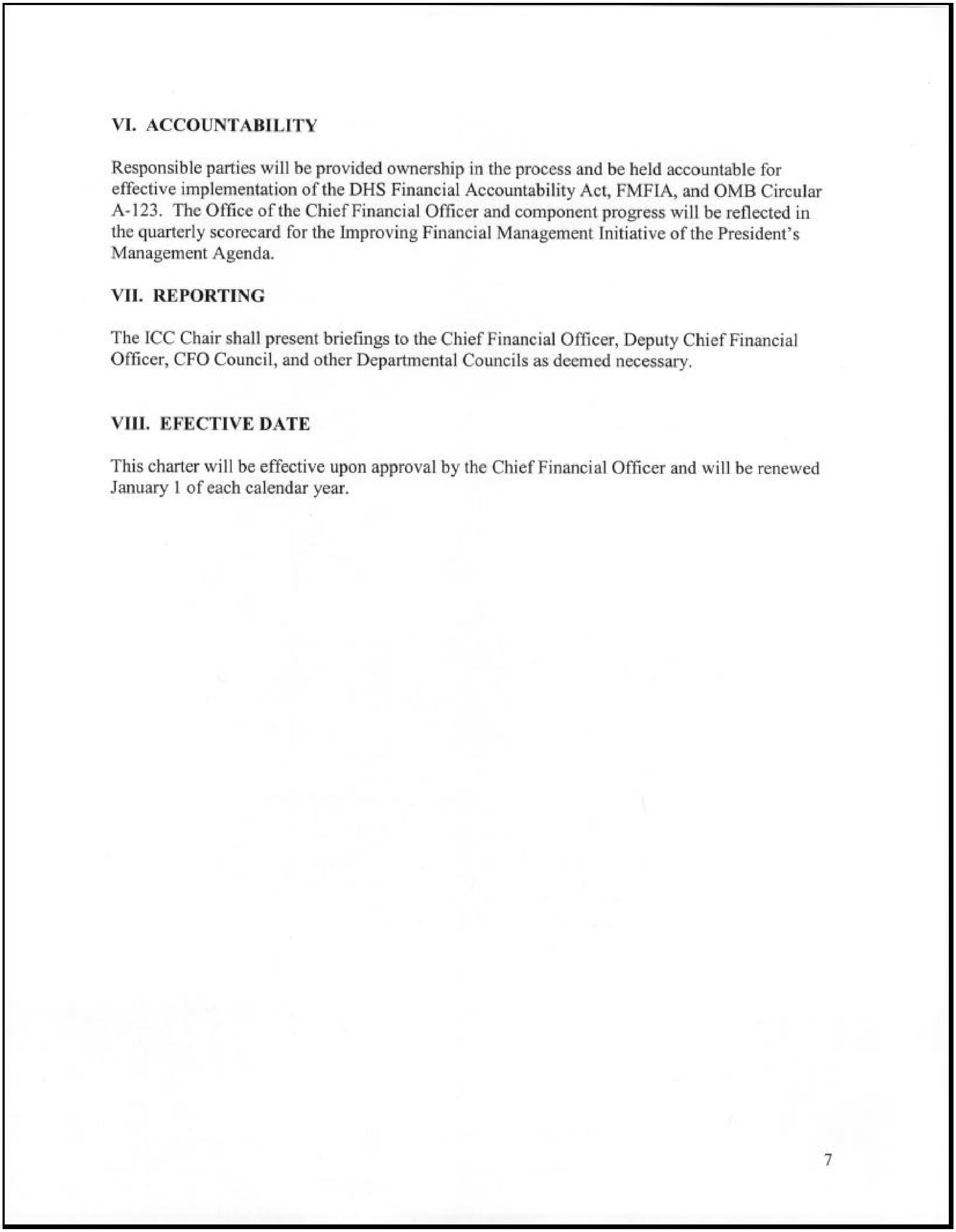
The organizational element representatives who serve as members of the Senior Assessment Team are authorized to execute the conditions of this Charter and are required to establish component level assessment teams. Assessment Teams are not required for assessments of internal controls other than financial reporting. However, components are encouraged to develop constructs that facilitate the integration and coordination of all internal-control assessments and activities.

Each organizational element will carry out its activities in a coordinated, mutually beneficial manner. Senior Assessment Team Core Membership includes senior executives and or senior staff from the following organizational elements:

- Information Analysis and Infrastructure Protection (IAIP);
- Border and Transportation Security (BTS);
- U.S. Customs and Border Protection (CBP);
- U.S. Immigration and Customs Enforcement (ICE);
- Transportation Security Administration (TSA);
- Federal Law Enforcement Training Center (FLETC);
- Office of State and Local Government Coordination and Preparedness, (SLGCP);
- Emergency Preparedness and Response (EPR);
- Science &Technology Directorate (S&T);
- U.S. Coast Guard (CG);
- U.S Citizenship and Immigration Services (CIS);
- United States Secret Service (SS); and
- Office of Inspector General (Administration)

V. MEETINGS

Meetings of the Senior Management Council and Senior Assessment Team will be held as necessary. Meetings of the ICC will be held preferably bi-weekly, but may be held as deemed necessary. Minutes and agendas of meetings will be documented and distributed.



VI. ACCOUNTABILITY

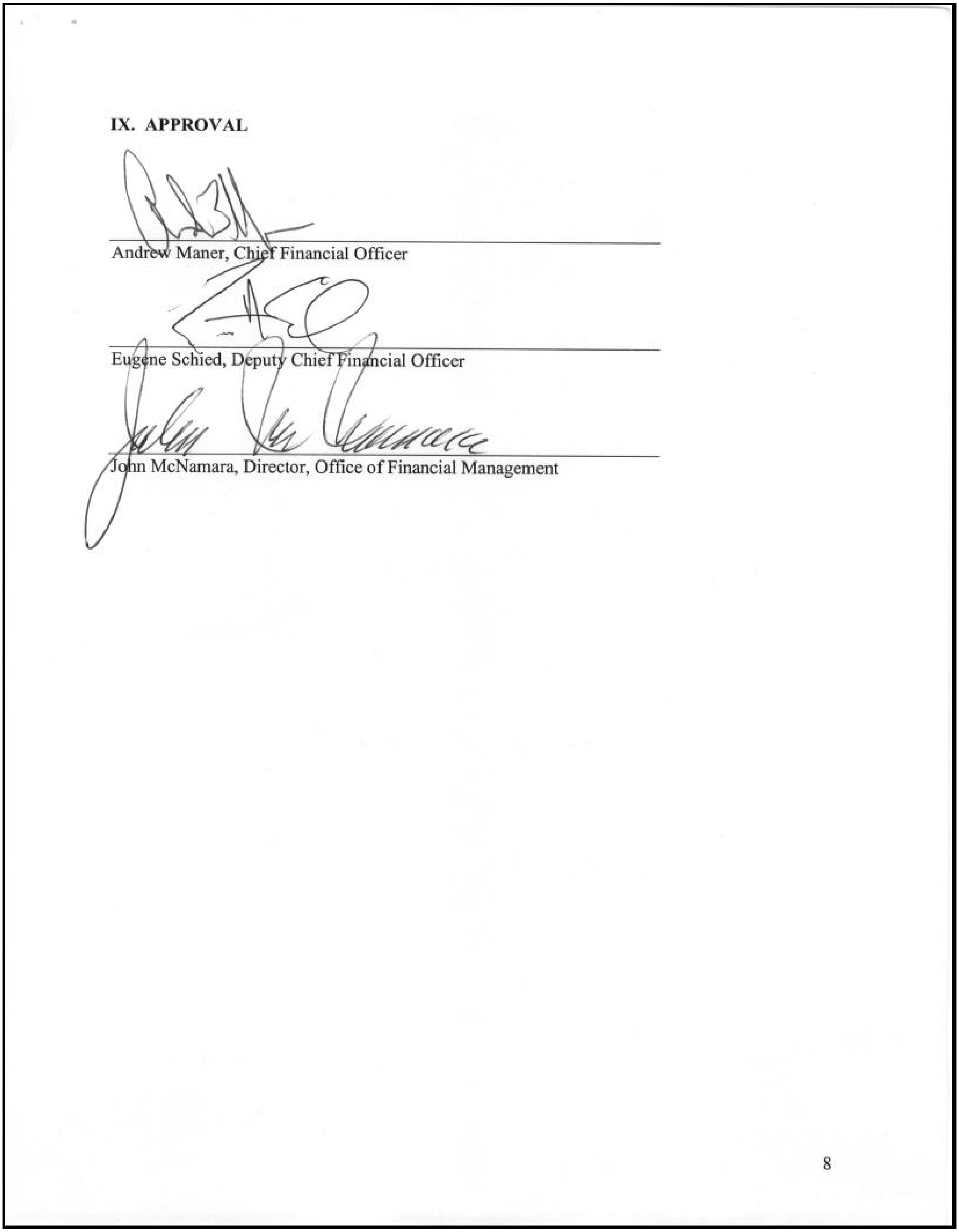
Responsible parties will be provided ownership in the process and be held accountable for effective implementation of the DHS Financial Accountability Act, FMFIA, and OMB Circular A-123. The Office of the Chief Financial Officer and component progress will be reflected in the quarterly scorecard for the Improving Financial Management Initiative of the President's Management Agenda.

VII. REPORTING

The ICC Chair shall present briefings to the Chief Financial Officer, Deputy Chief Financial Officer, CFO Council, and other Departmental Councils as deemed necessary.

VIII. EFECTIVE DATE

This charter will be effective upon approval by the Chief Financial Officer and will be renewed January 1 of each calendar year.



IX. APPROVAL

Andrew Maner, Chief Financial Officer

Eugene Schied, Deputy Chief Financial Officer

John McNamara, Director, Office of Financial Management

Appendix D – Index of Definitions and Key Terms

This implementation guide uses many key terms when discussing how management must evaluate its internal control over financial reporting.

Adjusted Exposure

Gross exposure (see definition below) multiplied by the upper limit deviation rate.

Application Controls

Automated control procedures (e.g., calculations, posting to accounts, generation of reports, edits, control routines, etc.) or manual controls that are dependent on IT (e.g., the review by an inventory manager of an exception report when the exception report is generated by IT). When IT is used to initiate, authorize, record, process, or report transactions or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for significant accounts or disclosures or may be critical to the effective functioning of manual controls that depend on IT.

Automated Controls

Automated controls encompass those control procedures performed by a computer.

Compensating Controls

Controls that operate at a level of precision that would result in the prevention or detection of a misstatement that was more than inconsequential or material, as applicable, to annual or interim financial statements. The level of precision should be established considering the possibility of further undetected misstatements.

Complementary Controls

Controls that function together to achieve the same control objective.

Component

Formerly referred to as bureaus, or operational elements, or distinct Departmental offices within the agency.

Component Assessment Team[61]

The assessment team at the Component level. The team should be comprised of staff at the Component level and derive its authority and support from Component leadership, to include the Component Chief Financial Officer. The Component assessment team lead is the respective core member of the Senior Assessment Team.

[61] Based on recommendation provided in OMB Circular A-123 page 24.

Control Deficiency

A deficiency in the design or operation of a control that does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- A deficiency in *design* exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if it operates as designed, the control objective is not always met.
- A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

Control Objective

The objective(s) related to internal control over financial reporting to achieve the assertions that underlie an organization's financial statements.

De minimis

The full expression is **de minimis non curat lex**. This is a Latin phrase which means "the law does not care about very small matters". It can be used to describe a Component part of a wider transaction, where it is in itself insignificant or immaterial to the transaction as a whole, and will have no legal relevance or bearing on the end result.

Design Effectiveness

Internal control over financial reporting is designed effectively when the controls in place would meet the control objectives and be expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements.

Detective Control

Detective controls have the objective of detecting errors or fraud that has already occurred that could result in a misstatement of the financial statements.

Entity-Level Controls

Entity-level controls are controls management has in place to provide assurance that appropriate controls exist throughout the organization, including at the individual locations or operational units. Entity-level controls include[62]:

- Controls within the control environment, including tone at the top, the assignment of authority and responsibility, consistent policies and procedures, and entity-wide initiatives, such as codes of conduct and fraud prevention
- Management's risk assessment process
- Centralized processing and controls

[62] PCAOB AS 2.

- Controls to monitor other controls, including the activities of the OIG, senior management, and self-assessment programs
- The period-end financial reporting process
- Approved policies that address the entity's significant control and risk management practices

Financial Reporting[63]

Includes annual financial statements of an agency as well as significant internal and external financial reports that could have a material effect on a significant spending, budgetary or other financial decision of the agency or that is used to determine compliance with laws and regulations on the part of the agency.

Financial Statement Assertions

Management and the IPA must document and test internal control over relevant financial statement assertions. Financial statement assertions are defined as representations by management that are embodied in the financial statement Components and can be classified in the following broad categories[64]:

- Existence or Occurrence: This assertion addresses whether assets or liabilities of the entity exist at a given date and whether recorded transactions have occurred during a given period.
- Completeness: This assertion addresses whether all transactions and accounts that should be presented in the financial statements are so included.
- Valuation or Allocation: This assertion addresses whether asset, liability, equity, revenue, and expense Components have been included in the financial statements at appropriate amounts.
- Rights and Obligations: This assertion addresses whether assets are the rights of the entity and liabilities are the obligations of the entity at a given date.
- Presentation and Disclosure: This assertion addresses whether particular Components of the financial statements are properly classified, described, and disclosed.

Additionally, A-123 defines three additional assertions:

- The transactions are in compliance with applicable laws and regulations (compliance).
- All assets have been safeguarded against fraud and abuse.
- Documentation of internal control, all transactions, and other significant events is readily available for examination.

Although the financial statement assertions appear to be similar to the information processing objectives/ CAVR, there is not a one-for-one relationship, and they are used for different purposes. Information processing objectives/CAVR are used to evaluate the design effectiveness of controls, particularly application controls, within a process. Assertions are representations by management as to the fair presentation of the financial statements.

[63] OMB Circular A-123, page 22.

[64] Ibid.

General Computer Controls

General computer controls are one of the types of information processing controls included in the internal control Component of control activities. These are the processes and procedures that are used to manage and control an entity's information technology activities and computer environment. The Federal Information System Controls Audit Manual (FISCAM) was created by the Government Accountability Office (GAO) as the primary tool used by agencies within the federal government to evaluate their IT controls. Chapter three of FISCAM: "Evaluating and Testing General Controls" describes six major categories of general controls that should be considered. These are:

Figure 32: General Computer Controls

Category	Definition	Sub-Components (Critical Elements)
Entity-wide Security Program Planning and Management (SP), FISCAM section 3.1	The processes and controls used by an entity to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the computer-related controls.	■ Periodically assess risks ■ Document an entity-wide security program plan ■ Establish a security management structure and clearly assign security responsibilities ■ Implement effective security-related personnel policies ■ Monitor the security program's effectiveness and make changes as needed
Access Control (AC), FISCAM section 3.2	The processes and controls in place to ensure that access to system resources and data is authenticated and authorized to meet the entity's financial, operational, and compliance objectives.	■ Classify information resources according to their criticality and sensitivity ■ Maintain a current list of authorized users and their access authorized ■ Establish physical and logical controls to prevent or detect unauthorized access ■ Monitor access, investigate apparent security violations, and take appropriate remedial action

Category	Definition	Sub-Components (Critical Elements)
Application Software Development and Change Control (CC), FISCAM section 3.3	Application Software Development The processes and controls used by an entity to develop, configure, and implement new applications in order to meet the entity's financial, operational, and compliance objectives. This process is often referred to as the Software Development Lifecycle. Change Control The processes and controls used by an entity to ensure that modifications to programs continue to meet the entity's financial, operational, and compliance objectives.	■ Processing features and program modifications are properly authorized ■ Test and approve all new and revised software ■ Control software libraries
System Software (SS), FISCAM section 3.4	The processes and controls used by an entity to limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system	■ Limit access to system software ■ Monitor access to and use of system software ■ Control system software changes
Segregation of Duties (SD), FISCAM section 3.5	The processes and controls used by an entity to help ensure that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.	■ Segregate incompatible duties and establish related policies ■ Establish access controls to enforce segregation of duties ■ Control personnel activities through formal operating procedures and supervision and review
Service Continuity (SC), FISCAM section 3.6	The processes and controls used by an entity to ensure that when unexpected events occur (i.e., disaster, service interruption, or loss of data), critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.	■ Assess the criticality and sensitivity of computerized operations and identify supporting resources ■ Take steps to prevent and minimize potential damage and interruption ■ Develop and document a comprehensive contingency plan ■ Periodically test the contingency plan and adjust it as appropriate

Gross Exposure

A worst-case estimate of the magnitude of amounts or transactions exposed to the deficiency with regard to annual or interim financial statements, without regard to the upper limit deviation rate or likelihood of misstatement, and before considering complementary, redundant, or compensating controls. Factors affecting gross exposure include:

- The annual or interim financial statement amounts or total transactions exposed to the deficiency.
- The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current annual or interim period or that is expected in future periods.

Inconsequential

- Potential misstatements equal to or greater than 20% of overall annual or interim financial statement materiality are presumed to be more than inconsequential.
- Potential misstatements less than 20% of overall annual or interim financial statement materiality may be concluded to be more than inconsequential as a result of the consideration of qualitative factors, as required by AS 2.

Information Processing Objectives/CAVR

The four information processing objectives (completeness, accuracy, validity, and restricted access – sometimes referred to as "CAVR") are a standard means to assess the integrity of the data that flows through a process. The four Components of CAVR are listed below.

Figure 33: Information Processing Objectives/CAVR

Information Processing Objective	Definition
Completeness	■ All recorded transactions are accepted by the system (only once). ■ Duplicate postings are rejected by the system. ■ Any transactions that are rejected are addressed and fixed.
Accuracy	■ Key data elements for transactions (including standing data) that are recorded and input to the computer are correct. ■ Changes in standing data are accurately input.
Validity	■ Transactions, including the alteration of standing data, are authorized. ■ Transactions, including standing data files, are not fictitious and they relate to the organization.
Restricted Access	■ Unauthorized amendments of data are barred from the system. ■ The confidentiality of data is ensured. ■ Entity assets are physically protected from theft and misuse. ■ The segregation of duties is ensured.

Although control activities that achieve the information processing objectives do not always provide us with direct comfort on financial statement assertions, the table below may be useful in linking our controls work to the financial statement assertions, assuming that the process/sub-process to which the controls relate is designed effectively.

Figure 34: Linking Controls Work to Financial Statement Assertions[65]

Information Processing Objective	Financial Statement Assertion
Completeness	Completeness, Existence/Occurrence
Accuracy	Valuation/Allocation
Validity	Existence/Occurrence, Rights & Obligations
Restricted Access	Most, except for Rights & Obligations

Why is it that restricted access links to most assertions?

Restricted access to assets and records means that data is protected against unauthorized amendments, its confidentiality is ensured, and physical assets are protected. This is similar to the control environment or tone at the top in that it links to many of our assertions. If we know that the physical assets are protected, then we have contributed to our "existence/occurrence" assertion. If we know that access to the system is restricted, then we may have contributed to our "existence/occurrence", "completeness" and "valuation" assertions.

Internal Control[66]

An integral Component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding of assets

Internal Control over Financial Reporting

A process designed by, or under the supervision of, the agency head and chief financial officers, and effected by senior management, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements and other reports for internal and

[65] PwC Audit Guide.

[66] GAO Standards for Internal Control in the Federal Government (Green Book), page 6.

external purposes. This process involves the maintenance of records; the recording of transactions; and the prevention/detection of unauthorized acquisition, use, or disposition of the entity's assets[67].

Internal control over financial reporting should assure the safeguarding of assets from waste, loss, unauthorized use, or misappropriation as well as assure compliance with laws and regulations pertaining to financial reporting[68].

Internal Control Standards[69]

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires the Government Accountability Office (GAO) to issue standards for internal control in government. These standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement. These standards define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency's operations: programmatic, financial, and compliance. The GAO has identified and defined the five standards of internal control as follows:

1. **Control Environment –** management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

2. **Risk Assessment** – internal control should provide for an assessment of the risks the agency faces from both external and internal sources.

3. **Control Activities** – internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's control objectives.

4. **Information and Communications** – information should be recorded and communicated to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities.

5. **Monitoring –** internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

Locations or Component Units

The majority of companies are comprised of more than one location or organizational unit. The definition of a location or an organizational unit will depend on the nature of the entity. A location may be a legal entity (e.g., Department, agency), a division, a reporting unit, or an operational facility (e.g., border station, regional office). When completing management's assessment, significant judgment must be applied in assessing the definition of a location or an organizational unit to ensure appropriate planning of the project.

[67] Adapted from PCAOB AS 2.

[68] OMB Circular A-123, page 22.

[69] GAO Standards for Internal Control in the Federal Government (Green Book), page 3 - 9.

Management Assertions[70]

Agency management is required to include an assurance statement on the internal controls over financial reporting in its annual Performance and Accountability Report. This statement is based on management's assessment of the effectiveness of the agency's internal control over financial reporting.

Management Controls

Management controls are the organization, policies, and procedures used by agencies to reasonably ensure that (i) programs achieve their intended results; (ii) resources are used consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported and used for decision making.

Manual Controls

Manual controls encompass those controls performed manually, not by computer systems.

Material Weakness

1. **FMFIA overall** – reportable conditions which the agency head determines to be significant enough to report outside of the agency.

2. **Financial reporting** – a reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected in a timely manner.

Materiality[71]

The risk of error or misstatement that could occur in a financial report that would impact management's or users' decisions or conclusions based on such report.

Operational Effectiveness

Internal control over financial reporting is operating effectively when a properly designed control is operating as designed and the individual performing the control possesses the necessary authority and qualifications to perform the control effectively.

Opinion on Internal Control [72]

The auditor's opinion on internal control is based upon the auditor's evaluation of the entity's internal control and the results of other audit procedures. The opinion may be unqualified, unqualified with reference to reportable conditions, qualified, or adverse. Additionally, there may be restrictions on the scope of the procedures that result in a qualified opinion or a disclaimer of opinion.

[70] OMB Circular A-123, page 29.

[71] OMB Circular A-123, page 23.

[72] GAO/PCIE Financial Audit Manual, Sec. 500.38.

Beginning with fiscal year 2006, the Department of Homeland Security Financial Accountability Act requires the Department's annual PAR to include an audit opinion of the Department's internal controls over its financial reporting. CFO Act agencies generally receive a report on internal control which is not the same as an opinion.

Pervasive Controls other than GCC

The general programs and controls within the control environment, risk assessment, monitoring, and information and communication, including portions of the financial reporting process, that have a pervasive impact on controls at the process, transaction, or application level.

Potential Misstatement

An estimate of the misstatement that could result from a deficiency with a more than remote likelihood of occurrence.

Preventive Control

Preventive controls have the objective of preventing errors or fraud from initially occurring that could result in a misstatement of the financial statements.

Process or Cycle

A process or cycle is any sequence of transactions that enables an entity to complete tasks and achieve its objectives. These transactions may range, in order of complexity, from performing simple activities (such as processing invoices), to managing key elements of operations (such as an inventory management system), to executing functional tasks (such as maintaining an organization's financial records), to cross-functional elements (such as the entity's human resources Department).

Process/Cycle Risk Assessment

As part of the scoping exercises, management must identify the primary processes/cycles. In order to evaluate the extent of documentation and testing over each process/cycle, management should perform a risk assessment of each process/cycle. This risk assessment involves the identification of relevant risks to achieving the financial reporting objectives related to each account affected by each process/cycle. Higher risk processes/cycles will be subject to a greater extent of documentation and testing.

Reasonable Assurance

The concept of reasonable assurance encompasses the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance.

Redundant Controls

Controls that achieve the same control objective.

Remote or Remote Likelihood

As defined in SFFAS No. 5, the term "remote" is used when the chance of the future event, or events, occurring is slight.

Report on Internal Control[73]

A report on internal control (in which no opinion is issued) is a by-product report, a report that provides a limited degree of assurance about internal control. When no opinion is issued, the report on internal control is not the primary objective of the engagement. If the purpose of the audit is not to render an opinion on internal control, the auditor should report material weaknesses and other reportable conditions in internal control, or state that no material weaknesses were found.

Reportable Condition

1. **FMFIA overall** – a control deficiency, or combination of control deficiencies, that in management's judgment, should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives.

2. **Financial reporting** – a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected.

Senior Assessment Team[74]

The team should be comprised of senior executives and derive its authority and support from the Secretary of Homeland Security and/or the Chief Financial Officer. The team could take many forms such as a financial management improvement committee or as a subset of the Senior Management Council. The senior assessment team is responsible for:

- Oversight of the assessment process;
- Ensuring that assessment objectives are clearly communicated throughout the agency;
- Ensuring that the assessment is carried out in a thorough, effective, and timely manner;
- Identifying and ensuring adequate funding and resources are made available;
- Identifying staff and/or securing contractors to perform the assessment;
- Determining the scope of the assessment, i.e., those financial reports covered by the assessment; and
- Determining the assessment design and methodology.

[73] GAO/PCIE Financial Audit Manual, Sec. 500.49.

[74] OMB Circular A-123, page 24.

Senior Management Council[75]

The council may be comprised of the Chief Financial Officer, Senior Procurement Executive, Chief Information Officer, and managers of other functional offices. The council's role is to assess and monitor deficiencies in internal control by carrying out the following actions:

- involvement in identifying and ensuring correction of systemic weaknesses relating to each council member's respective functions;
- making recommendations to the Secretary of Homeland Security as to which reportable conditions are deemed to be material weaknesses to the agency as a whole and should therefore be included in the annual FMFIA assurance statement and reported in the agency's PAR;
- responsible for overseeing the timely implementation of corrective actions related to material weaknesses; and
- providing assistance in determining when sufficient action has been taken to declare that a reportable condition or material weakness has been corrected.

Shared Services

Shared services, a form of "internal outsourcing," enables organizations to achieve economies of scale by creating a separate internal entity within the organization to perform specific redundant services, such as payroll, accounts payable, travel and expense processing. A typical shared services initiative takes advantage of enterprise applications and other technological developments, enabling the company to achieve further improvements to quality in processes, such as finance, accounting, procurement, IT, and human resources. At the core of shared services is the idea that new technologies offer organizations the opportunity to 1) make better use of scarce skills, 2) provide information and services more

Significant Account and Disclosure

An account or disclosure is significant if there is a more-than-remote likelihood that the account or disclosure could contain misstatements that individually, or when aggregated with others, could have a material effect on the financial statements, considering the risks of both overstatement and understatement.

Sub-process or Sub-cycle

A sub-process or sub-cycle is a group of transactions for which specific accounting procedures and controls are established by an entity's management. For example, a revenue and receivables process may include sub-processes, such as invoicing, pricing, or processing of receipts.

Test Objective

The design of the test of a control activity to determine whether the control is operating as designed, giving consideration to:

- The nature of the control and the definition of an exception;
- The frequency with which the control operates;

[75] OMB Circular A-123, page 14.

- The desired level of assurance in combination with the reliability of the control, for example, whether the control is designed to achieve the control objective alone or in combination with other controls; and
- The number of exceptions expected.

Upper Limit Deviation Rate

The statistically derived estimate of the deviation rate based on the sample results, for which there is a remote likelihood that the true deviation rate in the population exceeds this rate (refer to AICPA Audit and Accounting Guide, Audit Sampling).

Walkthrough

A walkthrough is the process in which a transaction is traced from origination through the entity's information systems until the transaction is reflected in the entity's financial reports. A walkthrough should encompass the entire process of initiating, authorizing, recording, processing, and reporting individual transactions and controls for each significant process, including controls to address the risk of fraud.

Appendix E – Glossary of Acronyms

Acronym	Full Title
AICPA	American Institute for Certified Public Accountants
ASB	Auditing Standards Board
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations
CXO	Collective Chiefs
DHS	Department of Homeland Security
FAR	Federal Acquisition Regulation
FASAB	Federal Accounting Standards Advisory Board
FASB	Financial Accounting Standards Board
FISCAM	Federal Information System Controls Audit Manual
FY	Fiscal year
GAAP	Generally Accepted Accounting Principles
GAO	Government Accountability Office
GCC	General Computer Controls
ICC	Internal Control Committee
IG	Inspector General
IPA	Independent Public Accountant
MD	Management Directive
OCASO	Office of the Chief Administrative Services Officer
OCFO	Office of the Chief Financial Officer
OCHCO	Office of Chief Human Capital Officer
OCIO	Office of the Chief Information Officer
OCPO	Office of the Chief Procurement Officer
OGC	Office of General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PAR	Performance and Accountability Report
PCAOB	Public Company Accounting Oversight Board
RSI	Required Supplementary Information
RSSI	Required Supplementary Stewardship Information
SAS	Statement of Accounting Standards
SEC	Securities and Exchange Commission
SFFAS	Statement of Federal Financial Accounting Standard
SOX	Sarbanes-Oxley Act of 2002

Appendix F – Examples of Processes/Cycles and Sub-Processes/Sub-Cycles

Figure 35: Examples of Processes/Cycles and Sub-Processes/Sub-Cycles

PROCESSES/CYCLES AND SUB-PROCESSES/SUB-CYCLES	
Budget Execution	
	Budget submission
	Appropriations
	Apportionment
	Allotment
	Commitment
	Obligation
	Expended
	Outlay
Inventory	
	Inventory master file maintenance
	Inventory quantity control
	Obsolete and inventory control
	Shipping activities
	Receiving activities
Purchasing	
	Vendor master file maintenance
	Requisitions
	Purchase orders
	Goods receipting
	Invoice processing
	Cash disbursements
Revenues	
	Customer master file maintenance
	Pricing and order processing
	Invoicing
	Cash application and receipts processing
	Revenue recognition
Payroll and Employee Benefits	
	Payroll and employee master file maintenance
	Time and attendance
	Processing payroll
	Pension and post retirement benefits
PP&E Spending and Maintenance	
	PP&E master file maintenance
	PP&E acquisition requests
	Depreciation

PROCESSES/CYCLES AND SUB-PROCESSES/SUB-CYCLES	
	Disposals
	Leases (operating, capital)
Financial Reporting (including period-end reporting)	
	Planning, budgeting, and management reporting
	General ledger maintenance
	Consolidation and adjusting, eliminating and consolidating entries
	Accounting policies and procedures
	Footnote support
	Account analysis and reconciliations
	Intragovernmental and intradepartmental accounts
	Adoption of new accounting pronouncements
Treasury and Risk Management	
	Appropriation Recording
	Cash Receipt
	Cash Disbursement
	Treasury Reporting
	Reconciliation
	Environmental exposures
Information Systems	
	Control environment
	Program development
	Access to programs and data (security access)
	Computer operations
Grants Management	
Other/Miscellaneous	
	Prepaids and other miscellaneous assets
	Other miscellaneous liabilities and accruals
	Miscellaneous other revenue and cost

Appendix G – Example of Financial Statement Mapping of Significant Accounts to Processes/Cycles

Figure 36: Example of Financial Statement Mapping of Significant Accounts to Processes/Cycles

Financial Statement Account	Consolidated Balance	Coverage	Percent Coverage	Corresponding Cycle	Corresponding Cycle	Corresponding Cycle
BALANCE SHEET, As of September 30, 200X						
Assets						
Fund Balance with Treasury				Appropriation Recording	Cash Receipts/ Cash Disbursements	Treasury Reporting
Investments				Treasury and risk management		
Accounts receivable, net				Earned Revenue		
Prepaid expenses				Purchasing	Financial reporting	
Liabilities						
Current portion of capital lease obligations				PP&E spending and maintenance		
Accounts payable				Purchasing	Financial reporting	
Accrued expenses				Purchasing	Financial reporting	
Accrued payroll				Purchasing	Financial reporting	Payroll and employee benefits
STATEMENT OF NET COST, for fiscal year ended September 30, 200X						
Earned revenues				Revenue		
Gross cost				Purchasing	Payroll and employee benefits	
Payroll				Payroll and employee benefits		
Supporting Technology Controls						
Control environment				Information systems		
Program development				Information systems		
Program changes				Information systems		
Access to programs and data (Security)				Information systems		
Computer operations				Information systems		

Financial Statement Account	Consolidated Balance	Coverage	Percent Coverage	Corresponding Cycle	Corresponding Cycle	Corresponding Cycle
Note 1. Summary of significant accounting policies						
Department has summarized its significant policies around ■ Principles of general ledger accounting ■ Management estimates and assumptions				Financial reporting		
Note 2. Non-Entity Assets						
Department discloses assets that do not legally belong to the Department (i.e. FBWT)				Financial reporting	Treasury and risk management	
Note 3: Fund Balance with Treasury						
Department discloses appropriated funds, trust, funds, special funds, etc.				Financial reporting	Treasury and risk management	
RSI and RSSI						
RSI and RSSI are included in mapping in each individual piece.				Financial reporting	various	

Appendix H – Example of Mapping Processes/Cycles and Sub-Processes/Sub-Cycles to Locations

Figure 37: Example of Mapping Processes/Cycles and Sub-Processes/Sub-Cycles to Locations

Process / Cycle	Reporting Unit	Sub-Process 1	Sub-Process 2	Sub-Process 3	Sub-Process 4	Sub-Process 5	Sub-Process 6	Sub-Process 7
Revenue	Operating Unit A	Customer master	Pricing	Order processing	Invoicing			Cash application
	Operating Unit B	Customer master		Order processing				
Inventory	Operating Unit A		Obsolescence				Master file	
	Operating Unit B	Quantity control		Shipping	Receiving			
Purchasing	Operating Unit A	Vendor maintenance	Requisitions	Purchase orders	Goods receipting	Invoice processing	Cash disbursements	
	Operating Unit B	Vendor maintenance	Requisitions	Purchase orders	Goods receipting	Invoice processing	Cash disbursements	
Treasury and Risk Management	Operating Unit A	Fund Balance management	Investment management			Legal	Environ-mental	
	Operating Unit B	Fund Balance management					Environ-mental	
PP&E Spending and Maintenance	Operating Unit A	Acquisition requests	Master file	Depreciation	Disposals	Leases	Physical maintenance	
	Operating Unit B	Acquisition requests	Master file	Depreciation	Disposals	Leases	Physical maintenance	
Payroll and Employee Benefits	Operating Unit A	Master file	Time and attendance	Processing payroll	Pension and post retirement			
	Operating Unit B	Master file	Time and attendance	Processing payroll				
Financial Reporting	Operating Unit A	Planning, budgeting and reporting	General ledger maintenance	Consolidation and related entries	Accounting policies and procedures	Footnotes	Account analysis and reconciliation	Journal entry processing
	Operating Unit B	Planning, budgeting and reporting	General ledger maintenance		Accounting policies and procedures	Footnotes	Account analysis and reconciliation	Journal entry processing
Information Systems	Operating Unit A	Change management	Physical and logical security	Operations				
	Operating Unit B	Change management	Physical and logical security	Operations				
Miscellaneous	Operating Unit A				Other assets	Other liabilities		Miscellaneous revenue and cost
	Operating Unit B				Other assets	Other liabilities		Miscellaneous revenue and cost

Appendix I – Example of a Process/Cycle Risk Assessment

Following is an example of how to perform a process/cycle risk assessment by sub-process/ sub-cycle:

1. Determine significant risk factors that should be evaluated for each sub-cycle.
2. Assess the risk level as high, medium, or low for each risk factor in each sub-cycle.
3. Assign an overall risk rating (high, medium, or low) for each sub-cycle based upon an average of the individual risk factors for that sub-cycle.

Figure 38: Examples of Individual Risk Factors

Impact on Financial Statements	Misstatement or lack of controls could result in material misstatement in financial reporting
Complexity of the Process	Complexity as a function of financial statement data compilation or technical knowledge involved in determination of financial statement amount
Volume of Transactions	Number of transactions in a given period
Centralization of the Process	Centralization and direct control of processes by upper management
Inherent Risk in the Process	Inherent risk of errors or irregularities due to fraud

The risk assessment is performed to prioritize the assessment of controls and maximize the effectiveness and efficiency of the project. Higher-risk cycles would normally be subject to more robust testing of all relevant assertions for each significant account, whereas lower-risk cycles would normally be subject to reduced testing. For example, for lower-risk cycles, the lower end of ranges for sample sizes may be used when performing tests, or testing may be performed earlier in the fiscal year. With respect to evaluations of the risk for each factor, interpretations of the three ratings (high, medium, and low) are:

Figure 39: Risk Factor Interpretations

High	The possibility of misstatement is high, or the balance has a material impact on the financial statements.
Medium	The possibility for misstatements in the given areas of the financial statements is moderate, or the process is subject to an average degree of error.
Low	The process is straightforward, and a misstatement in this area would have a minimal impact on the financial statements.

Based upon the risk assessment for each risk factor, an overall priority level for a given sub-cycle can be assessed. The Senior Assessment Team can look to the overall priority level to tailor the extent of testing that will be required in management's assessment of the relevant assertions for that sub-cycle.

Below is an example of how this evaluation may be documented (Note that a similar analysis would be performed for at least each individually important location):

Figure 40: Risk Assessment Documentation

RISK ASSESSMENT - Department							
		Impact on Financial Statements	**Complexity of process**	**Volume of transaction**	**Centralization of process**	**Inherent risk of process**	**Priority A = H, B = M, C = L**
Revenue & Receivables							
	Customer Master	Medium	Medium	Low	Medium	Medium	**B**
	Pricing	High	Medium	Low	Medium	Medium	**B**
	Earned Revenue Forecasting	High	High	Medium	High	High	**A**
	Order Entry	High	Medium	Medium	Medium	High	**A**
	Shipping	High	Medium	Medium	Low	Medium	**A**
	Service Invoicing	High	High	Medium	Medium	Medium	**A**
	Maintenance Invoicing	High	Medium	Medium	Medium	Medium	**A**
	Cash Receipt	High	Low	High	Medium	High	**A**
	Revenue Recognition	High	High	High	Medium	High	**A**
Purchasing & Payables							
	Vendor Maintenance	Low	Medium	Medium	High	High	**B**
	Requisitions	High	Medium	High	High	High	**A**
	Purchase Orders	High	Medium	High	High	High	**A**
	Goods Receipting	Medium	Low	Medium	High	Medium	**B**
	Invoice Processing	High	Low	High	High	Medium	**B**
	Cash Disbursements	High	Low	High	High	High	**A**
Treasury							
	Fund Balance Management	High	Low	High	High	High	**B**
	Investment Management	High	Low	Low	Low	High	**C**
Asset Management							
	Fixed Asset Additions	Low	Low	Low	Medium	Low	**C**
	Depreciation	Low	Low	Low	Medium	Low	**C**
	Physical Maintenance	Low	Low	Low	Medium	Medium	**C**
	Capital Leases	Medium	Medium	Low	High	High	**B**
	Asset Disposal	Low	Low	Low	Medium	Medium	**C**

RISK Assessment						
	Impact on Financial Statements	**Complexity of process**	**Volume of transaction**	**Centralization of process**	**Inherent risk of process**	**Priority A = H, B = M, C = L**
Payroll and Human Capital						
New Employee	Low	Low	Low	High	Medium	**C**
Change In Status	Low	Low	Low	High	Low	**C**
Compensation	High	Medium	High	High	Low	**B**
Payroll Calculation	Medium	Low	High	High	Medium	**C**
Payroll Disbursement	Medium	Low	High	High	Medium	**C**
Payroll Accounting	Medium	Medium	Medium	High	Medium	**B**
Benefits Administration	Low	Medium	Medium	High	Medium	**C**
General Ledger Accounting						
Journal Entry Processing	High	Low	High	High	Medium	**B**
Period Closing	High	Medium	Low	High	Medium	**B**
Consolidation	High	High	Low	High	Medium	**A**
Management Estimates	Medium	High	Medium	Medium	High	**A**
Intragovernmental Transactions	Medium	Medium	Low	High	Medium	**B**
Adjusting Entries	Medium	High	Low	Medium	High	**A**
Financial Reporting						
Financial Reporting	High	High	Low	Medium	High	**A**
Intragovernmental Balances	Low	Medium	Low	Medium	High	**A**
Directorate Reporting	Medium	Medium	Low	Medium	Medium	**B**
Subsequent Events	Low	Medium	Low	Medium	Medium	**B**
Preparation of Disclosures	Medium	High	Low	Low	High	**A**
Information Systems						
Control Environment	High	High	High	Medium	High	**A**
Program Development	High	High	High	Medium	High	**A**
Access to Programs and Data (Security)	None	High	Low	Low	Low	**C**
Computer Operations	None	High	High	Medium	High	**A**
Legal						
Litigation	Low	High	Low	Medium	High	**B**
Fraud Programs	Medium	High	Low	High	High	**A**
Commitments and Contingencies	Medium	Low	Low	Medium	Low	**B**

Appendix J – Flowchart Guidance

Guidelines for the preparation of flowcharts:

- **Structure of flowcharts:** Consistently following a standard layout for flowcharts ensures that each flowchart is logically structured and can be easily followed and understood. The following rules should be used to prepare flowcharts:

  - Keep the main flow of activities and controls in a vertical line down the middle of the flowchart.
  - To the left and right of the flowchart, add the main input and output documents and computer files.
  - The sequence of activities should flow from top to bottom.
  - Each flowchart should take up no more than one printed page. If a flowchart is larger than one page, activities should be grouped into higher-level processes and documented in separate flowcharts.

- **Content of flowcharts:** The detailed operations and controls that are associated with various processes can be documented in flowcharts, with each main activity in a given process being assigned its own chart. Given the amount of information contained within a series of flowcharts, it is important to make each flowchart easily understandable. Documentation at each level should contain a meaningful amount of information without providing too much data. For example:

  Level 1: Overview of the process containing each of the main activities
  Level 2: Breakdown of the main activities into sub-activities
  Level 3: More detailed description of the sub-activities

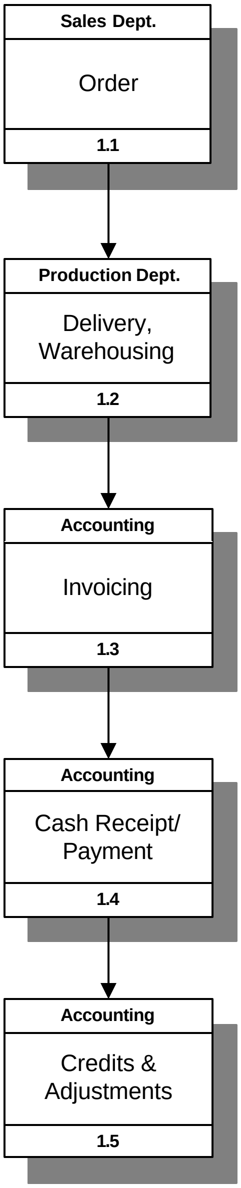
- **Common problems to avoid:**

  - *A set of flowcharts that describes every process in detail:* These charts become very difficult to read because there is little information on the higher levels.
  - *A highly complex single-level flowchart:* A flowchart of this sort may be difficult for the reader to understand.

The following flowcharts provide an executive-level overview of the revenue process and the cash application sub-process. In some cases, assessment teams may present more detailed flowcharts for the key sub-processes (i.e., Level 3).

Figure 41: Example of a Level 1 Flowchart – Sales Process

Process Flow & Controls Map



Description

1.1 Creation of sales order:

The creation of sales orders is initiated by a customer's order. The order management functions receive the order and enter all order data into the Sales and Accounts Receivable (SAR) system to create a sales order. The Sales Department creates the sales order in SAR by using a special item category in the sales order that automatically generates a delivery note.

1.2 Delivery and Warehousing:

Goods are picked for distribution from the warehouse and dispatched to the customer with the delivery note.

1.3 Invoicing:

Based on the completed delivery and related delivery note, billing to the customer takes place.

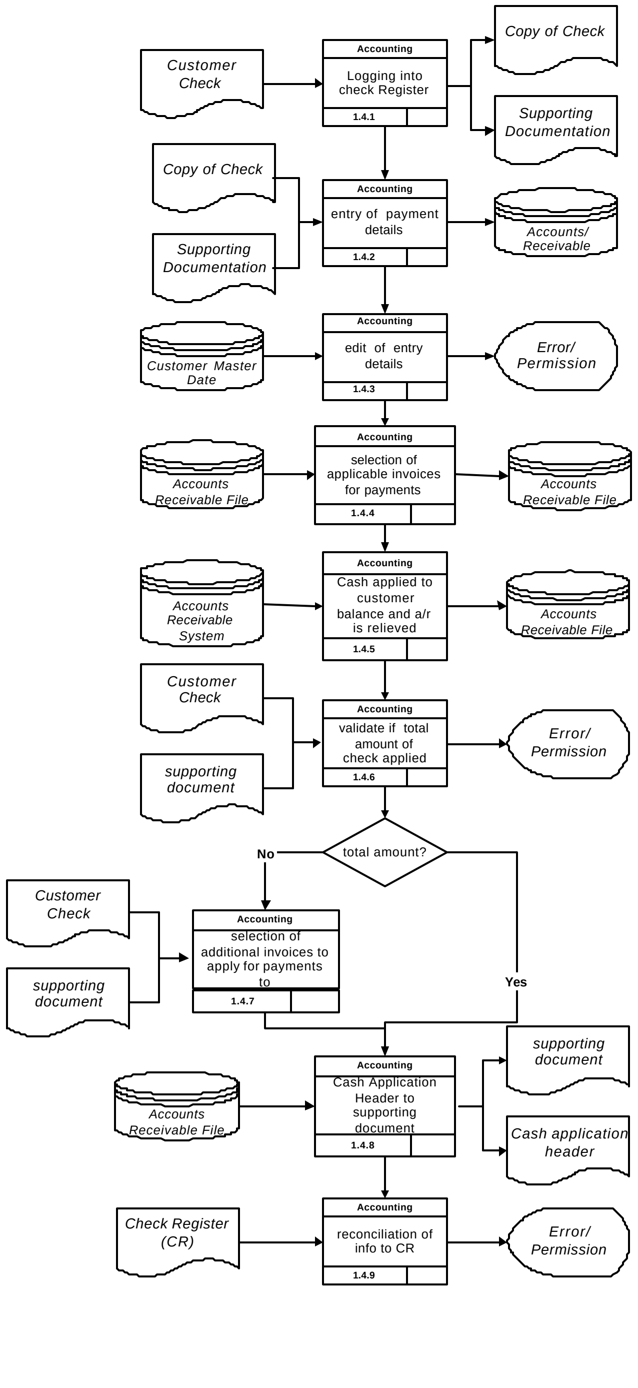
1.4 Cash Receipt:

The cash application process includes both manual and automated procedures. Cash received into the lockbox(s) is automatically applied to customer accounts via a Cash Receipts file that is created by the Cash Receipts System and sent to the mainframe computer system each night.

1.5 Credits and Adjustments:

Any required adjustments are made to customer accounts for returns, discounts, and other credits after required authorizations and supporting document are obtained.

Figure 42: Example of a Level 2 Flowchart – Cash Application Sub-process Showing Transactions and Controls

Process Flow & Controls Map	Description
	1.4.1 The checks are forwarded to the Accounting Supervisor who logs them in a Check Register. The information recorded includes date of check, check number, check amount, customer name/number, and invoices that payment relates to. The Accounting Supervisor makes copies of the checks and sends the check copies along with the invoice hard copy supporting documentation to the Accounts Receivable Department. 1.4.2 A representative of the AR Department (representative) enters the customer number into the Cash Application screen within the Accounts Receivable system. The system validates the customer number against the Customer Master (Standing Data) file within the system. 1.4.3 If the system does not find the number, an error message is displayed indicating the number is invalid. The representative has the option of entering the trading partner code or agency name into a search screen to locate the customer number. If the system locates the customer master record for the customer number entered, a list of open invoices is generated on to the screen. 1.4.4 The next screen is for the first invoice number selected to apply payment to. 1.4.5 The representative is prompted to enter the amount of payment being applied to the invoice on a field at the top of the screen. The amount will typically match the total invoice amount (listed on the bottom of the screen), but there are times that only partial payment is applied to a particular invoice. 1.4.6 The invoice amount entered must be numeric and cannot be for an amount greater than the amount left to apply from the payment. The representative scrolls through each invoice and applies cash to each applicable one. The system keeps a running total of the total amount of payment (per the check) and the amount left to be applied. 1.4.7 The representative cannot close out of the Cash Application screen without applying the total check amount to the open invoices. 1.4.8 The representative is responsible for scanning the Cash Application Header screen showing the high-level details of the cash application payment including check number, check amount, and check date. The representative posts the scanned Cash Application Header screen to the scanned check copy and supporting documentation. This information is uploaded to the AR System. 1.4.9 The Accounting Supervisor reconciles the documentation back to the Check Register to ensure all checks were applied.

Appendix K – Sample Control Evaluation

Following is an example of how to complete a process/cycle control evaluation form. The example represents a generic Fund Balance with Treasury process, and therefore does not include the details that would be available at the Component level.

Template Identification

The template must identify the following elements:

- Component
- Line Items being documented
- Related Accounts, All accounts affecting the related line item.
- Related Disclosures, All significant disclosures

Control Documentation

Instructions for completion of the Components of the template are as follows:

A. **Reference Number**: Include a reference number for each risk being documented.
B. **Process/Cycle**: Include the process/cycle being documented. Refer to appendix D, for definition of Process/Cycle.
C. **Sub process/Sub cycle**: Include the process/cycle being documented. Refer to appendix D, for definition of Sub process/Sub Cycle.
D. **Risks**: Include risks as follows:
    - **Control Risk**: Include the risk that a material misstatement that could occur in an assertion will not be prevented or detected and corrected on a timely basis by the entity's internal control[76].
    - **Inherit Risk**: Include risk of the entity susceptibility to financial reporting misstatements due to:
        - the nature of the entity's programs
        - the prior history of audit adjustments, or
        - the nature of material transactions and accounts[77]
    - **Fraud Risk**: Include risk of misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets[78].
    - **Compliance Risk**: Include the risks that transactions are in non-compliance with laws and regulations that have a direct and material effect on the financial statements.
E. **Control Objective**: Include objective of control that, if achieved, would provide the entity with reasonable assurance that identified risk will be mitigated and therefore misstatements (whether caused by error or fraud), losses, or noncompliance will be prevented or detected[79].
F. **Description and Frequency of Control Activities**: Include a description of the control activity implemented by management that addresses the control objective. As noted in Section 4.3 of the guide, at a minimum, control documentation must provide answers to the following questions:
    - **What** is the risk being controlled?

[76] Adopted from GAO/PCIE, Financial Audit Manual, section 260-Identify Risk Factors, Planning Phase

[77] Ibid

[78] Ibid

[79] Ibid

- **What** is the control activity?
- **Why** is the activity performed?
- **Who** (or what system) performs the control activity, including segregation of duties?
- **When** (how often) is the activity performed?
- **What** mechanism is used to perform the activity (reports and systems)?

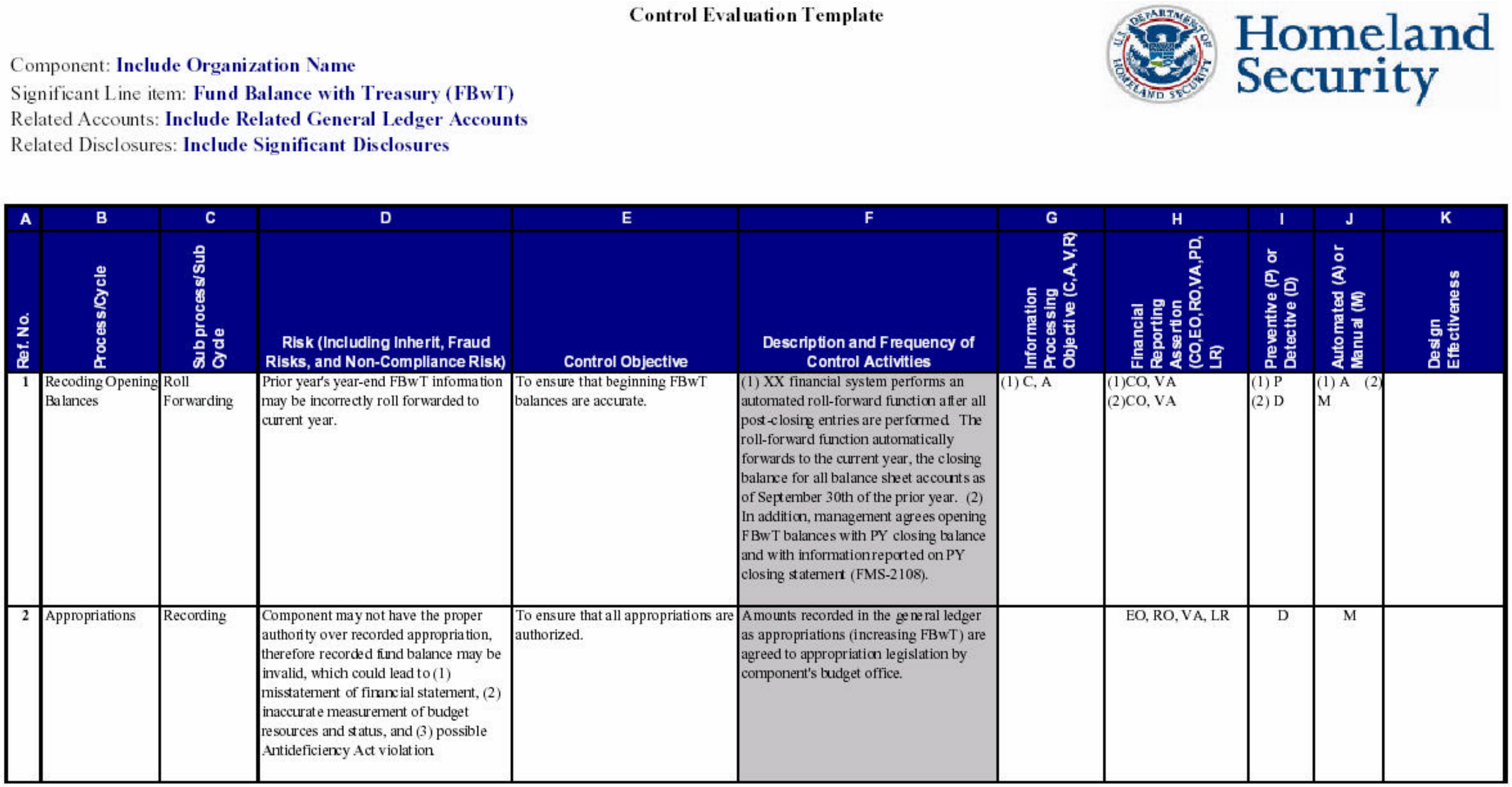
G. **Information Processing Objectives/CAVR**. Include the information processing objectives that are met by the control activity. Refer to appendix D, for definition of information processing objectives/CAVR and relationship to assertions.

H. **Financial Reporting Assertions**: Include the financial reporting assertions that are met by the control activity. Refer to appendix D, for definition of financial reporting assertions.

I. **Preventive or Detective Control:** Identify if the control is a preventive control (prevents a problem/misstatement) or detective control (detects a potential problem/misstatement after a transaction is executed).

J. **Automated or Manual:** Identify if the control is automated (computer controls) or manual (performed by an individual).

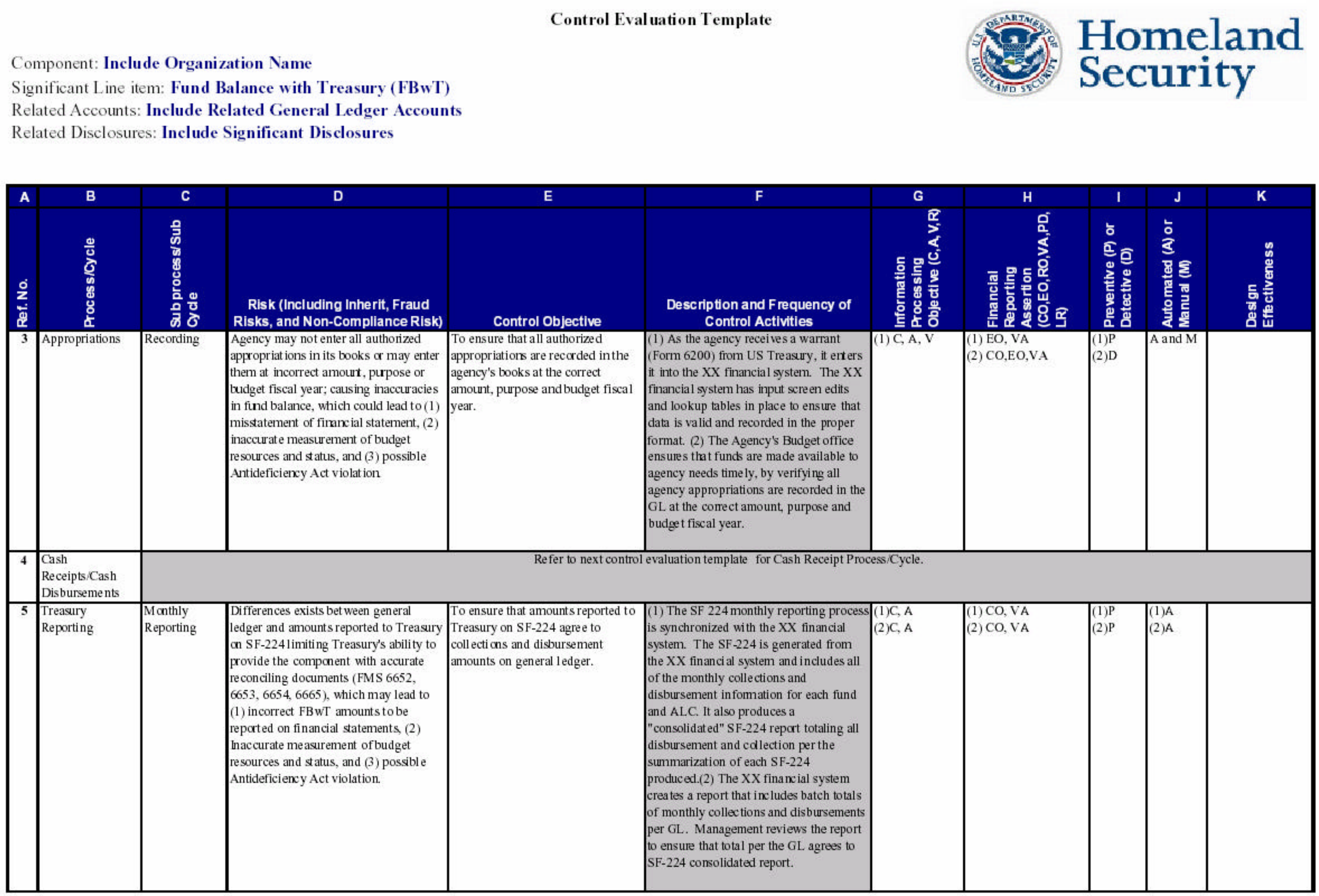
K. **Design Effectiveness:** Assess the design of the control (i.e. effective, moderately effective, not effective). Refer to Section 4.4 of the guide for guidance on how to assess the design of the controls.



Control Evaluation Template

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

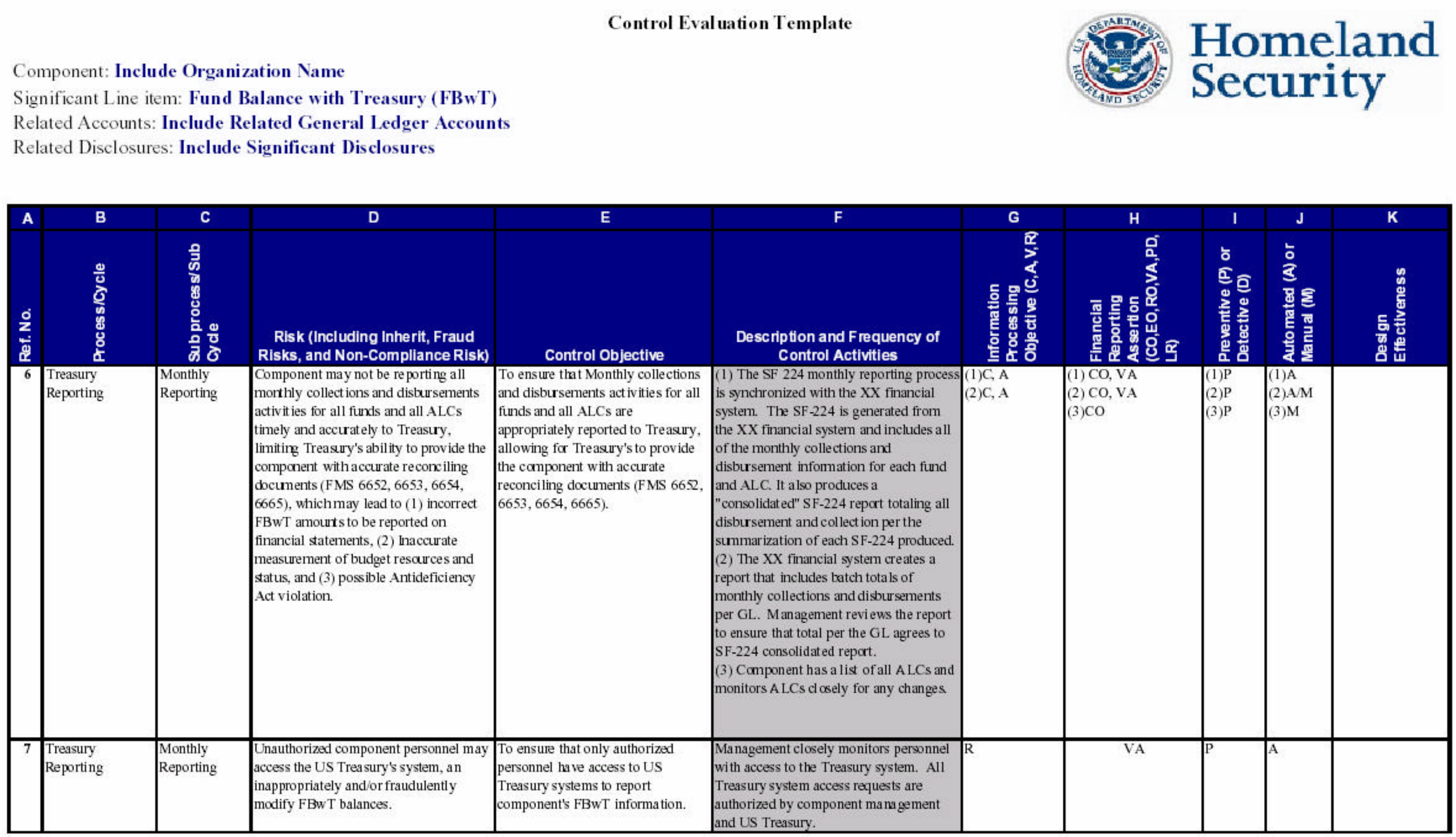
A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
1	Recoding Opening Balances	Roll Forwarding	Prior year's year-end FBwT information may be incorrectly roll forwarded to current year.	To ensure that beginning FBwT balances are accurate.	(1) XX financial system performs an automated roll-forward function after all post-closing entries are performed. The roll-forward function automatically forwards to the current year, the closing balance for all balance sheet accounts as of September 30th of the prior year. (2) In addition, management agrees opening FBwT balances with PY closing balance and with information reported on PY closing statement (FMS-2108).	(1) C, A	(1)CO, VA (2)CO, VA	(1) P (2) D	(1) A (2) M	
2	Appropriations	Recording	Component may not have the proper authority over recorded appropriation, therefore recorded fund balance may be invalid, which could lead to (1) misstatement of financial statement, (2) inaccurate measurement of budget resources and status, and (3) possible Antideficiency Act violation.	To ensure that all appropriations are authorized.	Amounts recorded in the general ledger as appropriations (increasing FBwT) are agreed to appropriation legislation by component's budget office.		EO, RO, VA, LR	D	M	



Control Evaluation Template

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

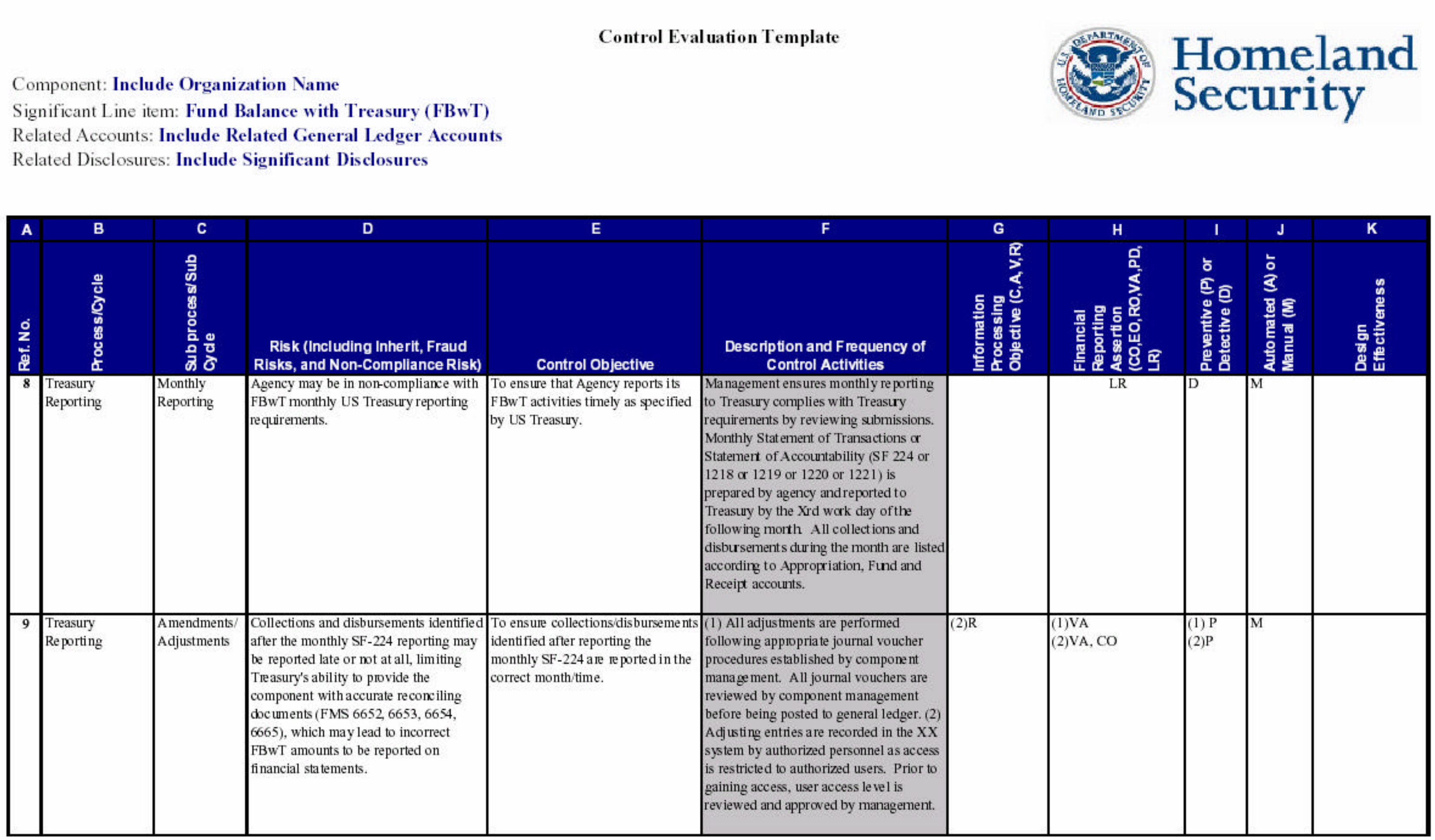
A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
3	Appropriations	Recording	Agency may not enter all authorized appropriations in its books or may enter them at incorrect amount, purpose or budget fiscal year; causing inaccuracies in fund balance, which could lead to (1) misstatement of financial statement, (2) inaccurate measurement of budget resources and status, and (3) possible Antideficiency Act violation.	To ensure that all authorized appropriations are recorded in the agency's books at the correct amount, purpose and budget fiscal year.	(1) As the agency receives a warrant (Form 6200) from US Treasury, it enters it into the XX financial system. The XX financial system has input screen edits and lookup tables in place to ensure that data is valid and recorded in the proper format. (2) The Agency's Budget office ensures that funds are made available to agency needs timely, by verifying all agency appropriations are recorded in the GL at the correct amount, purpose and budget fiscal year.	(1) C, A, V	(1) EO, VA (2) CO,EO,VA	(1)P (2)D	A and M	
4	Cash Receipts/Cash Disbursements	Refer to next control evaluation template for Cash Receipt Process/Cycle.								
5	Treasury Reporting	Monthly Reporting	Differences exists between general ledger and amounts reported to Treasury on SF-224 limiting Treasury's ability to provide the component with accurate reconciling documents (FMS 6652, 6653, 6654, 6665), which may lead to (1) incorrect FBwT amounts to be reported on financial statements, (2) Inaccurate measurement of budget resources and status, and (3) possible Antideficiency Act violation.	To ensure that amounts reported to Treasury on SF-224 agree to collections and disbursement amounts on general ledger.	(1) The SF 224 monthly reporting process is synchronized with the XX financial system. The SF-224 is generated from the XX financial system and includes all of the monthly collections and disbursement information for each fund and ALC. It also produces a "consolidated" SF-224 report totaling all disbursement and collection per the summarization of each SF-224 produced.(2) The XX financial system creates a report that includes batch totals of monthly collections and disbursements per GL. Management reviews the report to ensure that total per the GL agrees to SF-224 consolidated report.	(1)C, A (2)C, A	(1) CO, VA (2) CO, VA	(1)P (2)P	(1)A (2)A	



Control Evaluation Template

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

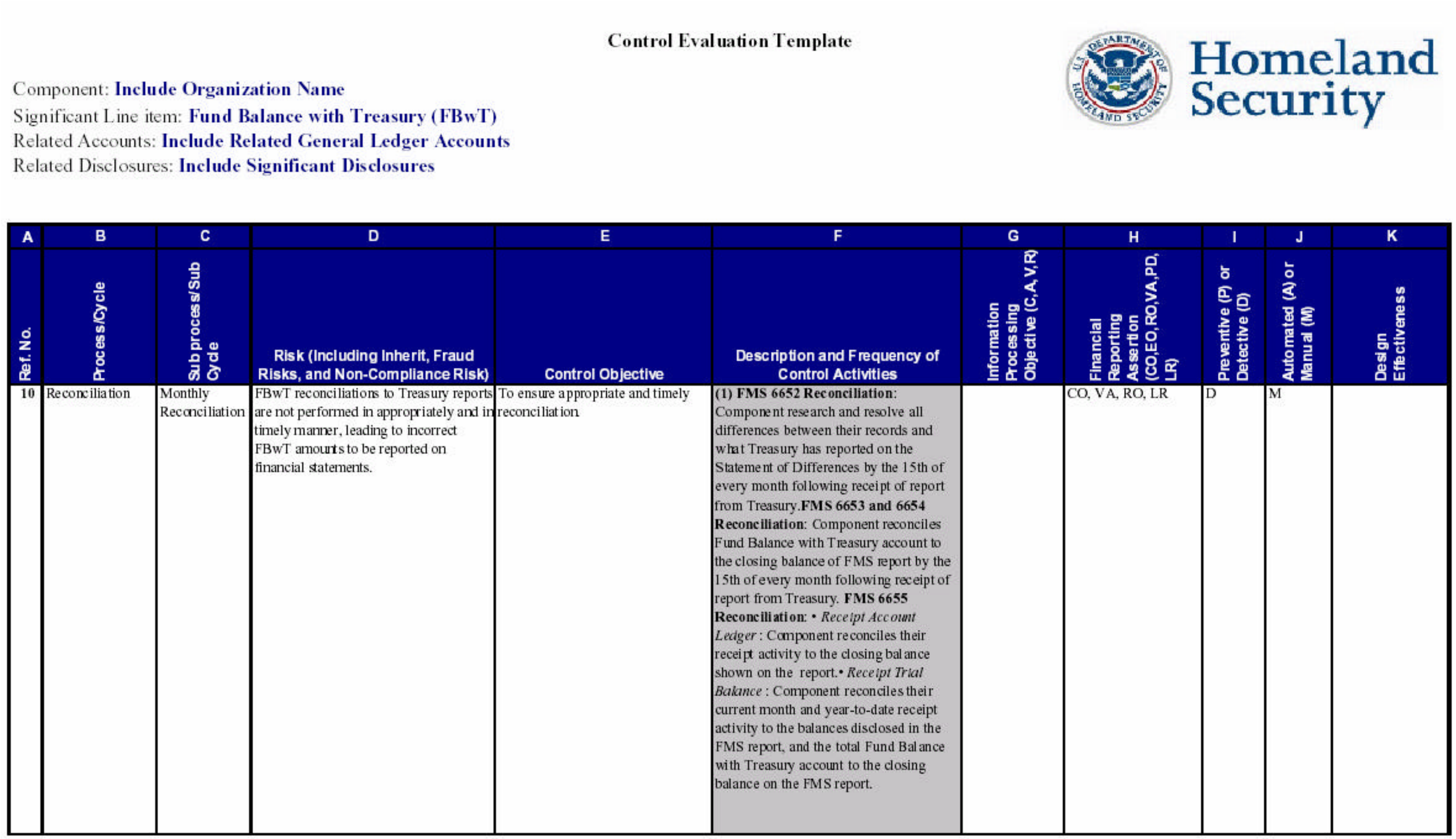
A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
6	Treasury Reporting	Monthly Reporting	Component may not be reporting all monthly collections and disbursements activities for all funds and all ALCs timely and accurately to Treasury, limiting Treasury's ability to provide the component with accurate reconciling documents (FMS 6652, 6653, 6654, 6665), which may lead to (1) incorrect FBwT amounts to be reported on financial statements, (2) Inaccurate measurement of budget resources and status, and (3) possible Antideficiency Act violation.	To ensure that Monthly collections and disbursements activities for all funds and all ALCs are appropriately reported to Treasury, allowing for Treasury's to provide the component with accurate reconciling documents (FMS 6652, 6653, 6654, 6665).	(1) The SF 224 monthly reporting process is synchronized with the XX financial system. The SF-224 is generated from the XX financial system and includes all of the monthly collections and disbursement information for each fund and ALC. It also produces a "consolidated" SF-224 report totaling all disbursement and collection per the summarization of each SF-224 produced. (2) The XX financial system creates a report that includes batch totals of monthly collections and disbursements per GL. Management reviews the report to ensure that total per the GL agrees to SF-224 consolidated report. (3) Component has a list of all ALCs and monitors ALCs closely for any changes.	(1)C, A (2)C, A	(1) CO, VA (2) CO, VA (3)CO	(1)P (2)P (3)P	(1)A (2)A/M (3)M	
7	Treasury Reporting	Monthly Reporting	Unauthorized component personnel may access the US Treasury's system, an inappropriately and/or fraudulently modify FBwT balances.	To ensure that only authorized personnel have access to US Treasury systems to report component's FBwT information.	Management closely monitors personnel with access to the Treasury system. All Treasury system access requests are authorized by component management and US Treasury.	R	VA	P	A	



Control Evaluation Template

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

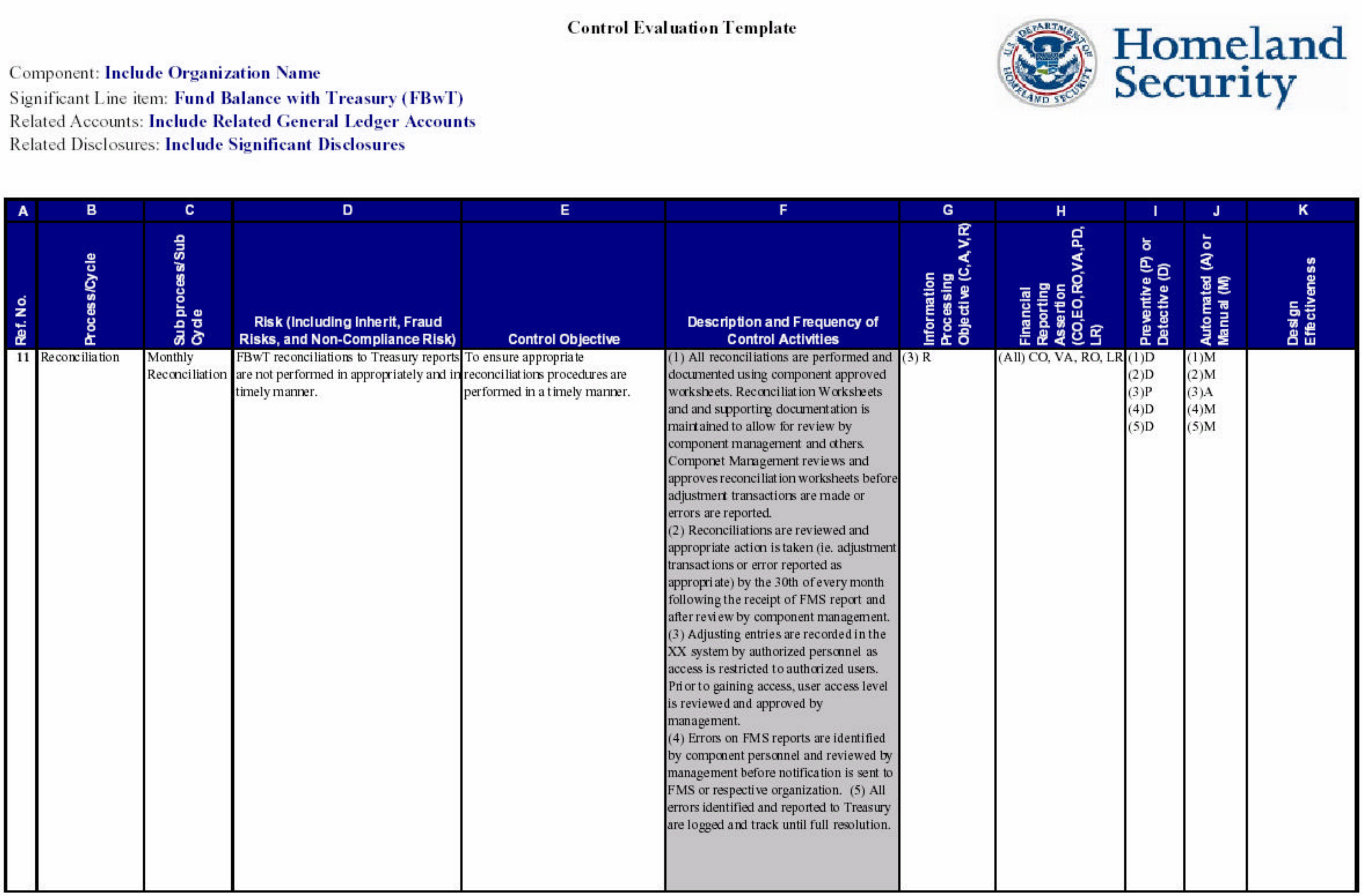
A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
8	Treasury Reporting	Monthly Reporting	Agency may be in non-compliance with FBwT monthly US Treasury reporting requirements.	To ensure that Agency reports its FBwT activities timely as specified by US Treasury.	Management ensures monthly reporting to Treasury complies with Treasury requirements by reviewing submissions. Monthly Statement of Transactions or Statement of Accountability (SF 224 or 1218 or 1219 or 1220 or 1221) is prepared by agency and reported to Treasury by the Xrd work day of the following month. All collections and disbursements during the month are listed according to Appropriation, Fund and Receipt accounts.		LR	D	M	
9	Treasury Reporting	Amendments/ Adjustments	Collections and disbursements identified after the monthly SF-224 reporting may be reported late or not at all, limiting Treasury's ability to provide the component with accurate reconciling documents (FMS 6652, 6653, 6654, 6665), which may lead to incorrect FBwT amounts to be reported on financial statements.	To ensure collections/disbursements identified after reporting the monthly SF-224 are reported in the correct month/time.	(1) All adjustments are performed following appropriate journal voucher procedures established by component management. All journal vouchers are reviewed by component management before being posted to general ledger. (2) Adjusting entries are recorded in the XX system by authorized personnel as access is restricted to authorized users. Prior to gaining access, user access level is reviewed and approved by management.	(2)R	(1)VA (2)VA, CO	(1) P (2)P	M	



Control Evaluation Template

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

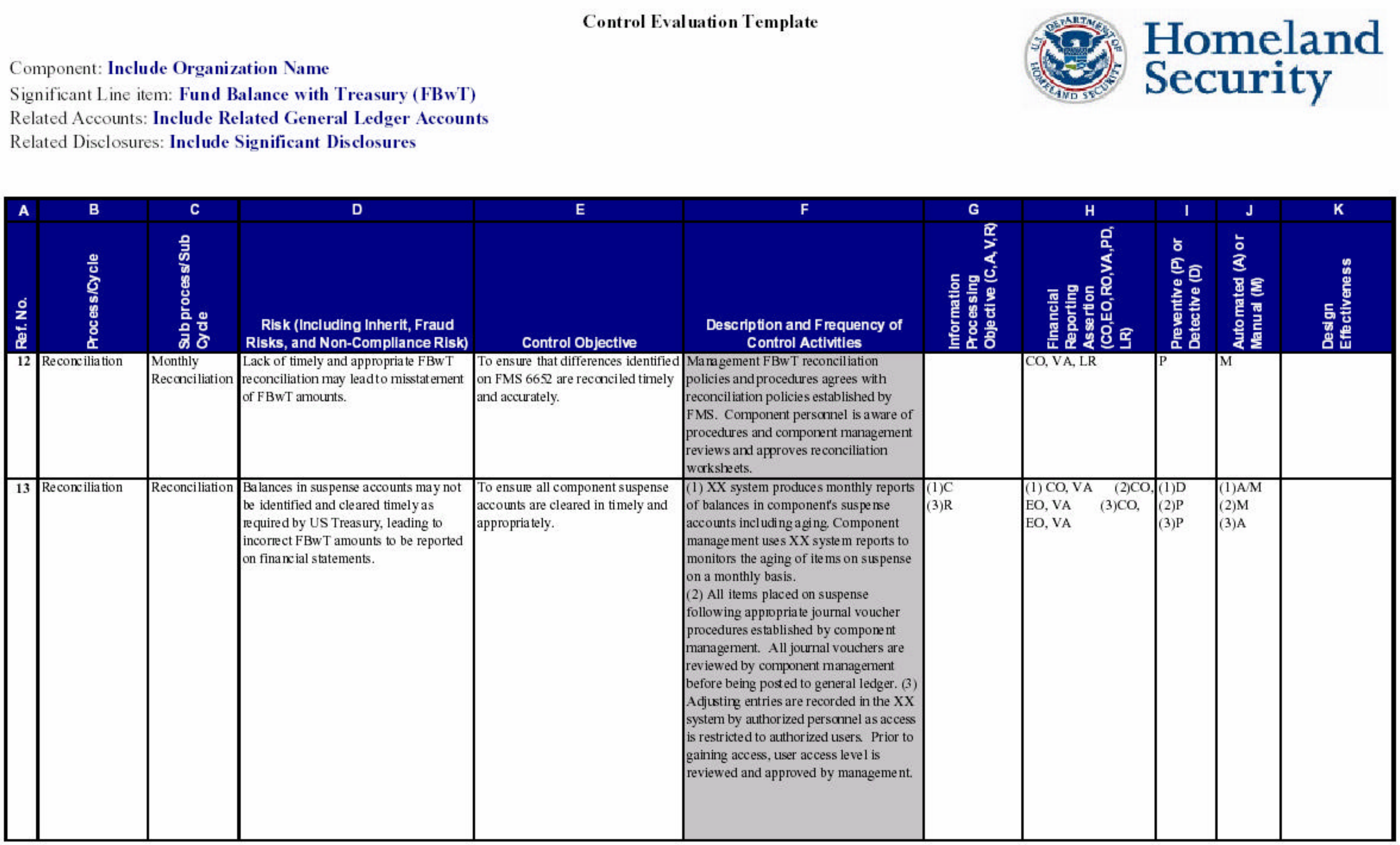
A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
10	Reconciliation	Monthly Reconciliation	FBwT reconciliations to Treasury reports are not performed in appropriately and in timely manner, leading to incorrect FBwT amounts to be reported on financial statements.	To ensure appropriate and timely reconciliation.	**(1) FMS 6652 Reconciliation**: Component research and resolve all differences between their records and what Treasury has reported on the Statement of Differences by the 15th of every month following receipt of report from Treasury.**FMS 6653 and 6654 Reconciliation**: Component reconciles Fund Balance with Treasury account to the closing balance of FMS report by the 15th of every month following receipt of report from Treasury. **FMS 6655 Reconciliation**: • *Receipt Account Ledger* : Component reconciles their receipt activity to the closing balance shown on the report.• *Receipt Trial Balance* : Component reconciles their current month and year-to-date receipt activity to the balances disclosed in the FMS report, and the total Fund Balance with Treasury account to the closing balance on the FMS report.		CO, VA, RO, LR	D	M	



Control Evaluation Template

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
11	Reconciliation	Monthly Reconciliation	FBwT reconciliations to Treasury reports are not performed in appropriately and in timely manner.	To ensure appropriate reconciliations procedures are performed in a timely manner.	(1) All reconciliations are performed and documented using component approved worksheets. Reconciliation Worksheets and and supporting documentation is maintained to allow for review by component management and others. Componet Management reviews and approves reconciliation worksheets before adjustment transactions are made or errors are reported. (2) Reconciliations are reviewed and appropriate action is taken (ie. adjustment transactions or error reported as appropriate) by the 30th of every month following the receipt of FMS report and after review by component management. (3) Adjusting entries are recorded in the XX system by authorized personnel as access is restricted to authorized users. Prior to gaining access, user access level is reviewed and approved by management. (4) Errors on FMS reports are identified by component personnel and reviewed by management before notification is sent to FMS or respective organization. (5) All errors identified and reported to Treasury are logged and track until full resolution.	(3) R	(All) CO, VA, RO, LR	(1)D (2)D (3)P (4)D (5)D	(1)M (2)M (3)A (4)M (5)M	



Control Evaluation Template

Homeland Security

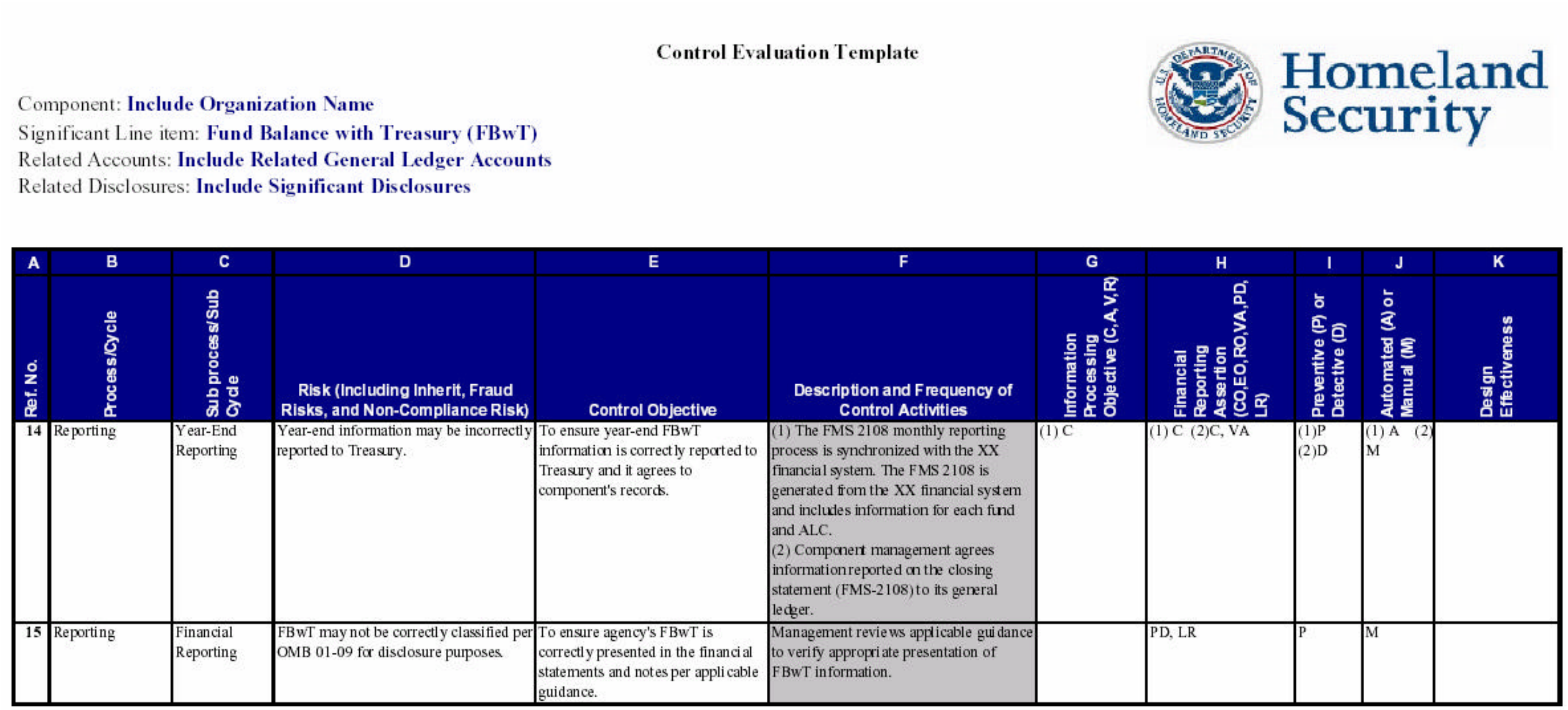
Component: **Include Organization Name**

Significant Line item: **Fund Balance with Treasury (FBwT)**

Related Accounts: **Include Related General Ledger Accounts**

Related Disclosures: **Include Significant Disclosures**

A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
12	Reconciliation	Monthly Reconciliation	Lack of timely and appropriate FBwT reconciliation may lead to misstatement of FBwT amounts.	To ensure that differences identified on FMS 6652 are reconciled timely and accurately.	Management FBwT reconciliation policies and procedures agrees with reconciliation policies established by FMS. Component personnel is aware of procedures and component management reviews and approves reconciliation worksheets.		CO, VA, LR	P	M	
13	Reconciliation	Reconciliation	Balances in suspense accounts may not be identified and cleared timely as required by US Treasury, leading to incorrect FBwT amounts to be reported on financial statements.	To ensure all component suspense accounts are cleared in timely and appropriately.	(1) XX system produces monthly reports of balances in component's suspense accounts including aging. Component management uses XX system reports to monitors the aging of items on suspense on a monthly basis. (2) All items placed on suspense following appropriate journal voucher procedures established by component management. All journal vouchers are reviewed by component management before being posted to general ledger. (3) Adjusting entries are recorded in the XX system by authorized personnel as access is restricted to authorized users. Prior to gaining access, user access level is reviewed and approved by management.	(1)C (3)R	(1) CO, VA (2)CO, EO, VA (3)CO, EO, VA	(1)D (2)P (3)P	(1)A/M (2)M (3)A	

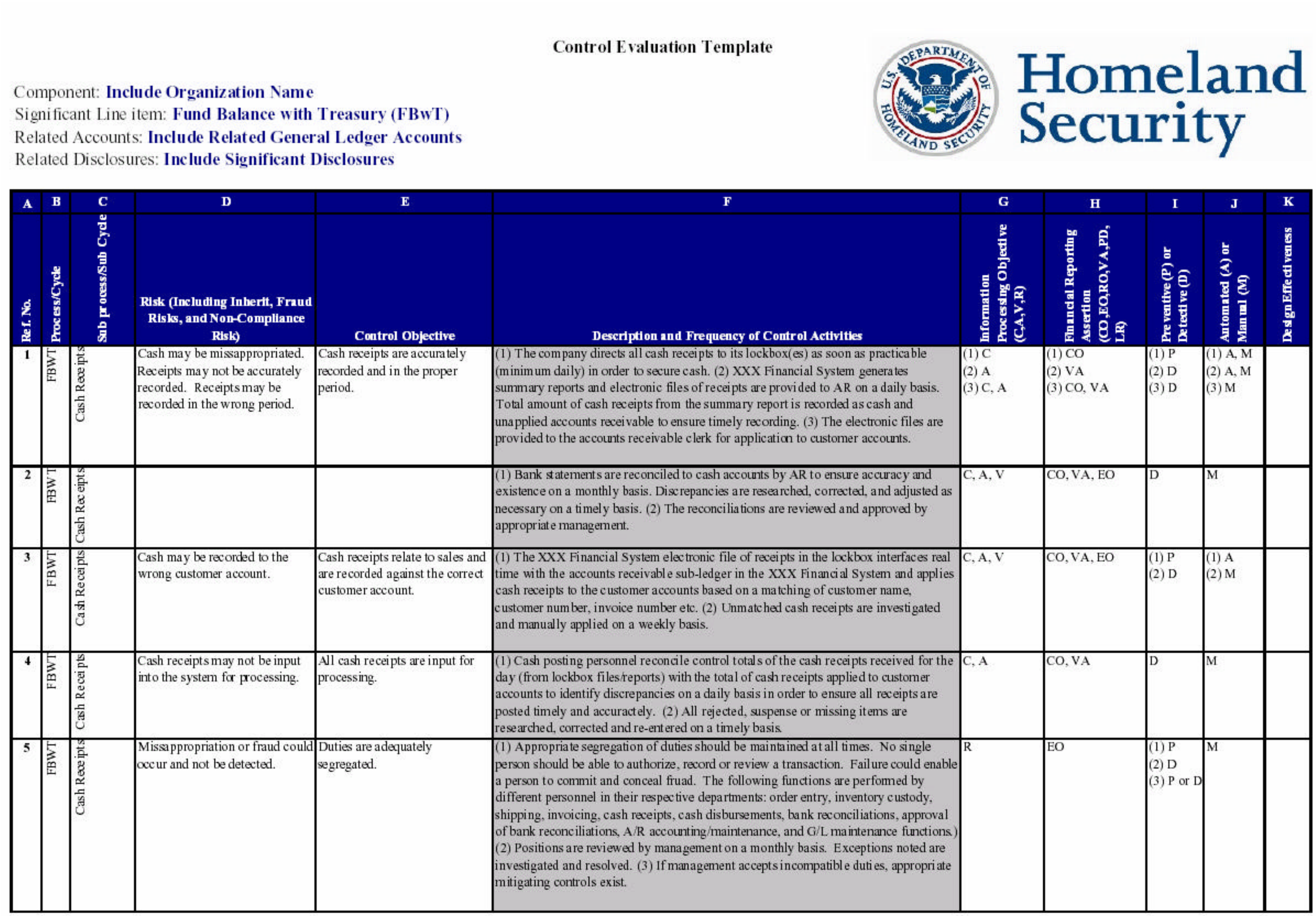


Control Evaluation Template

Homeland Security

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
14	Reporting	Year-End Reporting	Year-end information may be incorrectly reported to Treasury.	To ensure year-end FBwT information is correctly reported to Treasury and it agrees to component's records.	(1) The FMS 2108 monthly reporting process is synchronized with the XX financial system. The FMS 2108 is generated from the XX financial system and includes information for each fund and ALC. (2) Component management agrees information reported on the closing statement (FMS-2108) to its general ledger.	(1) C	(1) C (2)C, VA	(1)P (2)D	(1) A (2) M	
15	Reporting	Financial Reporting	FBwT may not be correctly classified per OMB 01-09 for disclosure purposes.	To ensure agency's FBwT is correctly presented in the financial statements and notes per applicable guidance.	Management reviews applicable guidance to verify appropriate presentation of FBwT information.		PD, LR	P	M	

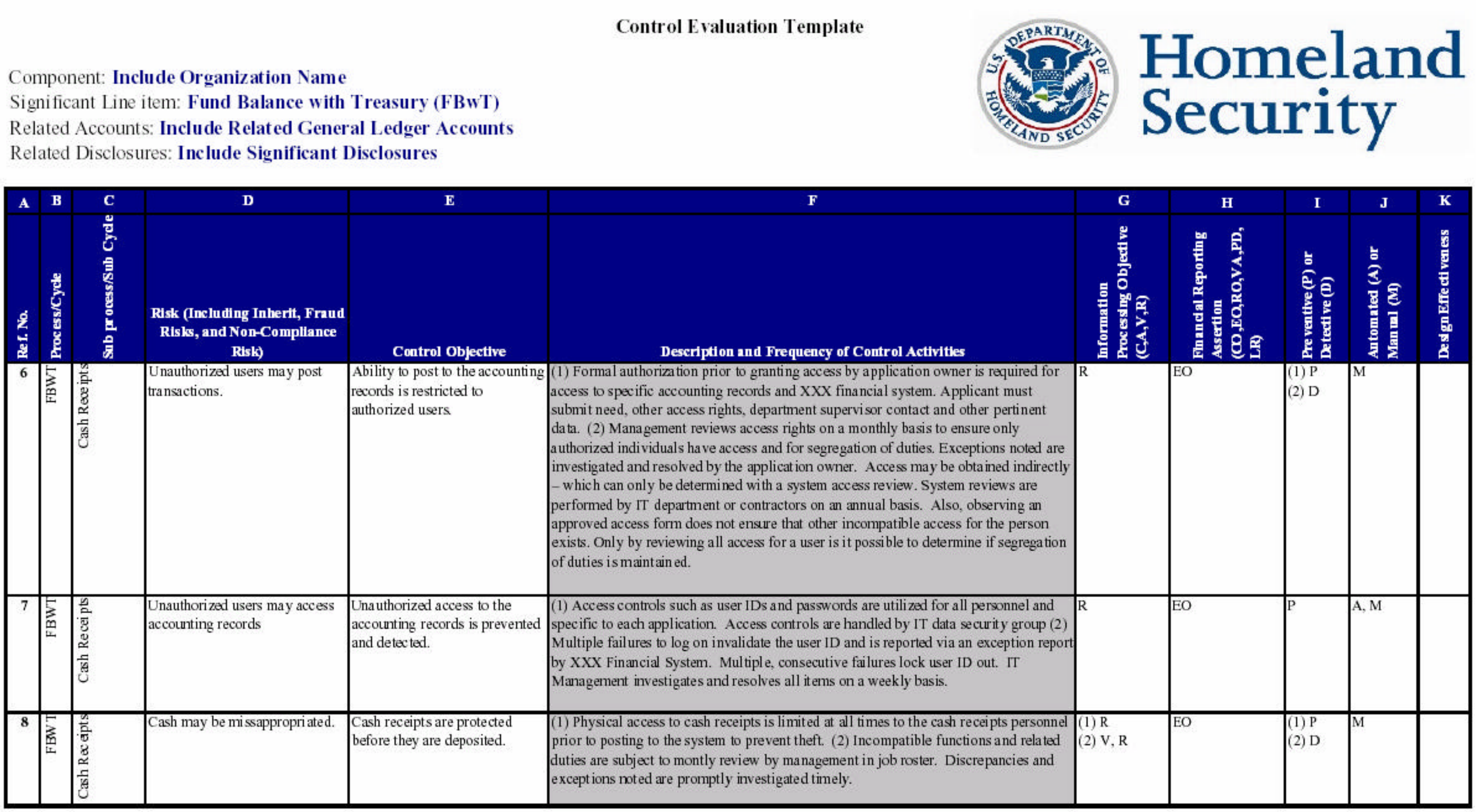


Control Evaluation Template

Homeland Security

Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
1	FBWT	Cash Receipts	Cash may be missappropriated. Receipts may not be accurately recorded. Receipts may be recorded in the wrong period.	Cash receipts are accurately recorded and in the proper period.	(1) The company directs all cash receipts to its lockbox(es) as soon as practicable (minimum daily) in order to secure cash. (2) XXX Financial System generates summary reports and electronic files of receipts are provided to AR on a daily basis. Total amount of cash receipts from the summary report is recorded as cash and unapplied accounts receivable to ensure timely recording. (3) The electronic files are provided to the accounts receivable clerk for application to customer accounts.	(1) C (2) A (3) C, A	(1) CO (2) VA (3) CO, VA	(1) P (2) D (3) D	(1) A, M (2) A, M (3) M	
2	FBWT	Cash Receipts			(1) Bank statements are reconciled to cash accounts by AR to ensure accuracy and existence on a monthly basis. Discrepancies are researched, corrected, and adjusted as necessary on a timely basis. (2) The reconciliations are reviewed and approved by appropriate management.	C, A, V	CO, VA, EO	D	M	
3	FBWT	Cash Receipts	Cash may be recorded to the wrong customer account.	Cash receipts relate to sales and are recorded against the correct customer account.	(1) The XXX Financial System electronic file of receipts in the lockbox interfaces real time with the accounts receivable sub-ledger in the XXX Financial System and applies cash receipts to the customer accounts based on a matching of customer name, customer number, invoice number etc. (2) Unmatched cash receipts are investigated and manually applied on a weekly basis.	C, A, V	CO, VA, EO	(1) P (2) D	(1) A (2) M	
4	FBWT	Cash Receipts	Cash receipts may not be input into the system for processing.	All cash receipts are input for processing.	(1) Cash posting personnel reconcile control totals of the cash receipts received for the day (from lockbox files/reports) with the total of cash receipts applied to customer accounts to identify discrepancies on a daily basis in order to ensure all receipts are posted timely and accuractely. (2) All rejected, suspense or missing items are researched, corrected and re-entered on a timely basis.	C, A	CO, VA	D	M	
5	FBWT	Cash Receipts	Missappropriation or fraud could occur and not be detected.	Duties are adequately segregated.	(1) Appropriate segregation of duties should be maintained at all times. No single person should be able to authorize, record or review a transaction. Failure could enable a person to commit and conceal fruad. The following functions are performed by different personnel in their respective departments: order entry, inventory custody, shipping, invoicing, cash receipts, cash disbursements, bank reconciliations, approval of bank reconciliations, A/R accounting/maintenance, and G/L maintenance functions.) (2) Positions are reviewed by management on a monthly basis. Exceptions noted are investigated and resolved. (3) If management accepts incompatible duties, appropriate mitigating controls exist.	R	EO	(1) P (2) D (3) P or D	M	



Control Evaluation Template

Component: Include Organization Name
Significant Line item: Fund Balance with Treasury (FBwT)
Related Accounts: Include Related General Ledger Accounts
Related Disclosures: Include Significant Disclosures

Homeland Security

A	B	C	D	E	F	G	H	I	J	K
Ref. No.	Process/Cycle	Sub process/Sub Cycle	Risk (Including Inherit, Fraud Risks, and Non-Compliance Risk)	Control Objective	Description and Frequency of Control Activities	Information Processing Objective (C,A,V,R)	Financial Reporting Assertion (CO,EO,RO,VA,PD, LR)	Preventive (P) or Detective (D)	Automated (A) or Manual (M)	Design Effectiveness
6	FBWT	Cash Receipts	Unauthorized users may post transactions.	Ability to post to the accounting records is restricted to authorized users.	(1) Formal authorization prior to granting access by application owner is required for access to specific accounting records and XXX financial system. Applicant must submit need, other access rights, department supervisor contact and other pertinent data. (2) Management reviews access rights on a monthly basis to ensure only authorized individuals have access and for segregation of duties. Exceptions noted are investigated and resolved by the application owner. Access may be obtained indirectly – which can only be determined with a system access review. System reviews are performed by IT department or contractors on an annual basis. Also, observing an approved access form does not ensure that other incompatible access for the person exists. Only by reviewing all access for a user is it possible to determine if segregation of duties is maintained.	R	EO	(1) P (2) D	M	
7	FBWT	Cash Receipts	Unauthorized users may access accounting records	Unauthorized access to the accounting records is prevented and detected.	(1) Access controls such as user IDs and passwords are utilized for all personnel and specific to each application. Access controls are handled by IT data security group (2) Multiple failures to log on invalidate the user ID and is reported via an exception report by XXX Financial System. Multiple, consecutive failures lock user ID out. IT Management investigates and resolves all items on a weekly basis.	R	EO	P	A, M	
8	FBWT	Cash Receipts	Cash may be missappropriated.	Cash receipts are protected before they are deposited.	(1) Physical access to cash receipts is limited at all times to the cash receipts personnel prior to posting to the system to prevent theft. (2) Incompatible functions and related duties are subject to montly review by management in job roster. Discrepancies and exceptions noted are promptly investigated timely.	(1) R (2) V, R	EO	(1) P (2) D	M	

Appendix L – General Computer Evaluation Template

Figure 43: General Computer Evaluation Template

FISCAM Reference	Critical Element (Control Objective)	Description and Frequency of Control Activity	Control Techniques	P or D (1)	A or M (2)	Control Effective (Y/N)?
SP-1	Periodically assess risks	Periodically assess risks	Independent risk assessments are performed and documented on a regular basis or whenever systems, facilities, or other conditions change. The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data. Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the security program plan, which is discussed in SP-2.)	P	M	
SP-2.1	Document an entity-wide security program plan	A security plan is documented and approved.	A security program plan has been documented that • covers all major facilities and operations, • has been approved by key affected parties, and • covers the topics prescribed by OMB Circular A-130 (general support systems / major applications), including: ➢ System and Application rules ➢ Training / Specialized training ➢ Personnel controls and security ➢ Incident response capability ➢ Continuity of support / Contingency planning ➢ Technical security and controls ➢ System interconnection / Information sharing ➢ Public access controls	P	M	
SP-2.2	Document an entity-wide security program plan	The plan is kept current.	The plan is reviewed periodically and adjusted to reflect current conditions and risks.	P	M	

Appendix M – Examples in Applying the Definitions of Significant Deficiency and Material Weakness

Weaknesses in the following areas would ordinarily be considered at least reportable conditions:

- Controls over the selection and application of accounting policies that are in conformity with GAAP
- Anti-fraud programs and controls
- Controls over non-routine or non-systematic transactions
- Controls over the period-end financial reporting process

Each of the following circumstances should be regarded as at least a reportable condition, and as a strong indicator that a material weakness exists:

- Restatement of previously issued financial statements to reflect the correction of a misstatement due to error or fraud.
- Identification by the auditor of a material misstatement in the financial statements in the current period that was not initially identified by the Department's internal control over financial reporting. (This would be a strong indicator of a material weakness even if management were to subsequently correct the misstatement.)
- Oversight of the Department's external financial reporting and internal control over financial reporting by the OIG and Senior Assessment Team is ineffective.
- The OIG and risk assessment function is ineffective where such a function needs to be effective for the Department to have an effective monitoring or risk assessment Component.
- An ineffective regulatory compliance function. This relates solely to those aspects of the ineffective regulatory compliance function in which associated violations of laws and regulations could have a material effect on financial reporting.
- Identification of fraud of any magnitude on the part of senior management.
- Reportable conditions that have been reported but remain uncorrected after some reasonable period of time.
- An ineffective control environment.

The following scenarios describe hypothetical situations that may help the Senior Assessment Team evaluate deficiencies as either reportable conditions or material weaknesses. The examples are adapted from the PCAOB's Auditing Standard No. 2*.*

Scenario A – Reportable Condition
The Department processes a significant number of routine interdepartmental transactions on a monthly basis. Individual transactions are not material and primarily relate to balance-sheet activity. A formal management

policy requires monthly reconciliation of interdepartmental accounts and confirmation of balances between Components. However, there is not a process in place to ensure that these procedures are performed. As a result, detailed reconciliations of interdepartmental accounts are not performed on a timely basis. Management does perform monthly procedures to investigate selected large-dollar differences between interdepartmental accounts. In addition, management prepares a detailed monthly variance analysis of operating expenses to assess their reasonableness.

Drawing only on these facts, the auditor should determine that this deficiency (i.e., the entity's failure to reconcile interdepartmental accounts on a timely basis) represents a reportable condition for the following reasons: It would be reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be more than inconsequential but less than material, because (1) individual interdepartmental transactions are not material and (2) the compensating controls (which operate monthly) should detect a material misstatement. Furthermore, the transactions are primarily restricted to balance-sheet accounts. However, the compensating detective controls are designed to detect material misstatements only. The controls do not address the detection of misstatements that are more than inconsequential but less than material. Thus there is a more-than-remote likelihood of a misstatement that is more than inconsequential but less than material.

Scenario B – Material Weakness

The Department processes a significant number of interdepartmental transactions on a monthly basis. Interdepartmental transactions relate to a wide range of activities, including transfers of inventory with interdepartmental profit between Components, allocation of costs to Components, and overhead charges. Individual interdepartmental transactions are frequently material. A formal management policy requires monthly reconciliation of interdepartmental accounts and confirmation of balances between Components. However, there is not a process in place to ensure that these procedures are performed on a consistent basis. As a result, reconciliations of interdepartmental accounts are not performed on a timely basis, and differences in interdepartmental accounts are frequent and significant. Management does not perform any alternative controls to investigate significant differences between interdepartmental accounts.

Using only these facts, the Senior Assessment Team should determine that this deficiency represents a material weakness for the following reasons: It is reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be material, because individual interdepartmental transactions are frequently material and relate to a wide range of activities. Additionally, actual unreconciled differences in interdepartmental accounts have been, and are, material. The likelihood of such a misstatement is more than remote because such misstatements have frequently occurred and compensating controls are not effective, either because they are not properly designed or they are not operating effectively. Taken together, the likelihood and potential magnitude of a financial-statement misstatement resulting from this internal-control deficiency meet the definition of a material weakness.

Scenario C – Material Weakness

During its assessment of internal control over financial reporting, Component assessment teams detected the deficiencies listed below. Based on the context in which the deficiencies occur, the Senior Assessment Team and the auditor agree that, individually, each of the following deficiencies represents a reportable condition:

- Inadequate segregation of duties pertaining to certain controls that govern access to the Department's information system.
- Several instances when transactions were not properly recorded within the subsidiary ledgers (transactions were not material, either individually or in the aggregate).

- A lack of timely reconciliations of the account balances that were affected by improperly recorded transactions.
- The same accounts are impacted by the second and third bullets.

Looking at these facts only, the Senior Assessment Team should determine that the combination of these reportable conditions represents a material weakness for the following reasons: The Senior Assessment Team ascertained that, individually, these deficiencies represent a more-than-remote likelihood of a misstatement that is more than inconsequential but less than material. However, each of these reportable conditions affects the same set of accounts. Taken together, these reportable conditions represent a more-than-remote likelihood that a material misstatement could not be prevented or detected. Therefore, in combination, these reportable conditions represent a material weakness.

Appendix N – DHS Corrective Action Plan (CAP) Form

Template Instructions

(1) Insert the date that you are submitting your quarterly update status report to the Department. **(Field 1 to 4)**
(2) Insert the Audit Finding Title. The title should correspond to the Consolidated Material Weakness in Internal Control as reported in Appendix I of the FY2004 Auditor's Report, Reportable Condition, or Control Deficiency. **(Field 5)**
(3) Provide an Audit Finding ID. In providing the audit finding ID, the first segment should correspond with the directorate/bureau code (e.g., OFM); the second segment should consist of the fiscal year the report was issued in (e.g., 04); the third segment should be the report letter issued by the auditor or Senior Assessment Team (e.g., A). **(Field 6)**
(4) If applicable, provide the related KPMG Notice of Finding and Recommendation (NFR) Title**(Field 7)**:
(5) If applicable, provide the related NFR number. **(Field 8)**
(6) Insert the date that this issue was first reported to the Department. For assistance, see the FY 2004 Consolidated Auditor's Report Appendix IV for a schedule on the Status of Prior Year Findings. **(Field 9)**
(7) Insert the original date that the issue was targeted to have been completed. **(Field 10)**
(8) If the date has been changed, insert the modified date that the issue is currently targeted to be completed by. **(Field 11)**
(9) Insert the organization responsible for the issue which is being reported. **(Field 12)**
(10) Insert a description of the issue (e.g., the condition). **(Field 13)**
(11) Describe all plans to resolve the issue being reported (i.e., What We Will Do About It) **(Field 14)**
(12) List all milestones planned to resolve the issue. **(Field 15)**
(13) If field 11 was changed during this reporting period, please note the reason for the change in the target completion date in. **(Field 16)**
(14) Describe how we will know the issue will be fixed. **(Field 17)**

U.S. DEPARTMENT OF HOMELAND SECURITY **Corrective Action Plan** **Issue and Milestone Schedule**	**DATES OF SUBMISSION**	
	First Quarter Update:	(Field 1)
	Second Quarter Update:	(Field 2)
	Third Quarter Update:	(Field 3)
	End of Year Report:	(Field 4)

Audit Finding Title: (Field 5)	**Audit Finding ID:** (Field 6)	**NFR Title (if applicable):** (Field 7)	**NFR # (if applicable):** (Field 8)

Date First Reported: (Field 9)	**Original Target Completion Date:** (Field 10)	**Current Target Completion Date:** (Field 11)	**Organization Responsible for Issue:** (Field 12)

Issue Description:
(Field 13)

What We Will Do About It (including all milestones):
(Field 14)

Milestones:	Original Target Date:	Current Target Date:	Actual Completion Date:
1: (Field 15)			
2:			
3:			
4:			
5:			
6: Insert additional Milestones if needed.			

Reasons for Change in Target Completion Date (if any):
(Field 16)

How We Will Know It is Fixed:
(Field 17)

Appendix O – Index, Point of Focus

Appendix P – The Five Standards of Internal Control

The Government Accountability Office (GAO) issues the *Standards for Internal Control in the Federal Government* commonly referred to as the "Green Book"[80]. These standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance challenges and areas at greatest risk for fraud, waste, abuse, and mismanagement.

As part of the assessment, the assessment team must document, test, and evaluate the design and effectiveness of the five standards of internal control. Because these standards form the foundation for all other controls implemented within an organization, it is important to document these controls during the planning phase of the assessment. Testing and evaluating these controls may be completed as part of the planning phase or during the very early stages of the testing phase. However, it is recommended that the testing and evaluation of these foundation controls occur as early in the assessment phase as possible. Weaknesses or deficiencies noted within these foundation controls will need to be remediated as soon as possible to prevent the weakening of other internal controls. Appendix P highlights the five Components of internal control and factors that the assessment team should consider when documenting, testing and evaluating these Components. Additional testing guidelines are provided within the testing section.

Control Environment

The control environment establishes the overall tone for the organization and is the foundation for all other Components of internal control. It provides discipline and structure as well as the climate which influences the quality of internal control[81]. The GAO identified seven sub-Components of the control environment:

- Integrity and ethical values
- Commitment to competence
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human capital policies and practices
- Relationship with Congress and central oversight groups (i.e., OMB, Inspector General, Senior Management Councils)

The assessment team must also address anti-fraud and abuse, programs and entity governance when evaluating the control environment[82].

Anti-Fraud and Abuse Considerations

Controls should be evaluated that are intended to address the risks of fraud and abuse and have at least a reasonably possible likelihood of having a material effect on the financial statements[83]. Abuse is distinct from

[80] Standards for Internal Control in the Federal Government, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

[81] Ibid.

[82] PCAOB AS 2.

[83] Ibid.

fraud. When abuse occurs, no law or regulation is violated. Rather, the conduct of a program or entity falls far short of behavior that is expected to be reasonable and necessary business practices by a prudent person[84].

Effective anti-fraud and abuse programs include the following key elements:

- Code of conduct/ethics
- Hotline/whistleblower program
- Hiring and promotion (i.e., background checks)
- Investigation and remediation of identified fraud
- Oversight
- Risk assessment

The assessment team should consider each of these elements in its documentation and evaluation of its anti-fraud and abuse program. Additionally, the assessment team's documentation should adequately support its assessment of anti-fraud programs and controls by:

- providing sufficient information regarding the flow of transactions, which enables management to determine where material misstatements could occur as a result of fraud;
- determining which controls prevent and detect fraud; and
- determining (1) who will perform the controls and (2) the related segregation of duties.

Risk Assessment

Another Component of internal control is risk assessment. For an organization to exercise effective control, it must establish clear, consistent objectives and understand the risks it faces in achieving those objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the Government Performance and Results Act, and forming a basis for determining how risks should be managed.[85]

The assessment team needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entity-wide and activity level. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments[86].

According to the Green Book, once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding how to manage the risk and what actions should be taken. The specific risk analysis methodology

[84] Adopted from the GAO Government Auditing Standards commonly referred to as the "Yellow-Book", paragraph 4.19.

[85] Adopted from the *Standards for Internal Control in the Federal Government*, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

[86] Ibid

used can vary by organization because of differences in organization's missions and the difficulty in qualitatively and quantitatively assigning risk levels. Because governmental, economic, industry, regulatory, and operating conditions continually change, mechanisms should be provided to identify and deal with any special risks prompted by such changes.

Management may address risk in a combination of the following ways:

- Having operating units perform risk assessments in a self-assessment format, which are then consolidated for review by a senior executive who is responsible for risk management or compliance with the DHS Financial Accountability Act and OMB Circular No. A-123
- Making a senior executive responsible for performing independent risk assessments
- Charging the Internal Control Committee Board with overseeing risk assessment
- Having the Office of Inspector General lead the assessment of fraud risk
- Holding weekly/monthly meetings of executive management to discuss key risks

Control Activities

Control activities are the policies and procedures that help to ensure that management's directives are implemented. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results[87]. Control activities occur throughout the organization, at all levels, and in all functions. The activities involve approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, maintenance of records, and segregation of duties.

There are many different types of control activities including preventive controls, detective controls, manual controls, computer controls, and internal controls. Control activities address specified information processing objectives/CAVR (completeness, accuracy, validity, and restricted access), such as ensuring completeness and accuracy of data processing. The following chart includes certain control activities that are commonly performed by personnel at various levels in organizations, as indicated by the Green Book.

Figure 44: Control Activities

Top Level Reviews of Actual Performance	Management should track major agency achievements and compare these to the plans, goals, and objectives established under the Government Performance and Results Act.
Reviews by Management at the Functional or Activity Level	Managers also need to compare actual performance to planned or expected results throughout the organization and analyze significant differences.
Management of Human Capital	Effective management of an organization's workforce, its human capital, is essential to achieving results and an important part of internal control. Management should view human capital as an asset rather than a cost. Only when the right personnel for the job

[87] Ibid

	are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved. Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization's success. As a part of its human capital planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.
Controls Over Information Processing	A variety of controls are performed to check accuracy, completeness, and authorization of transactions. Data entered into computer applications is subject to edit checks or matching to approved control files. An obligation, for example, is accepted only upon an approved requisition and availability of funds. Numerical sequences of transactions are accounted for. File totals are compared and reconciled with prior balances and with control accounts. Exceptions are investigated and reported to supervisors as necessary. Development of new systems and changes to existing systems are controlled, and access is checked to ensure the user performing the update is authorized to do so.
Physical Control Over Vulnerable Assets	An agency must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.
Establishment and Review of Performance Measures and Indicators	Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another, so analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.
Segregation of Duties	Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event. For example, a manager authorizing obligations would not be responsible for entering obligations into financial management systems or handling the payment of invoices.
Proper Execution of Transactions and Events	Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered into. Authorizations should be clearly communicated to managers and employees.
Accurate and Timely	Transactions should be promptly recorded to maintain their relevance and value to

Recording of Transactions and Events	management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.
Access Restrictions to and Accountability for Resources and Record	Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.
Appropriate Documentation of Transactions and Internal Control	Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained. These examples are meant only to illustrate the range and variety of control activities that may be useful to agency managers. They are not all inclusive and may not include particular control activities that an agency may need. Furthermore, an agency's internal control should be flexible to allow agencies to tailor control activities to fit their special needs. The specific control activities used by a given agency may be different from those used by others due to a number of factors. These could include specific threats they face and risks they incur; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

These examples are just a very few among a myriad of control procedures performed every day throughout an organization that serve to enforce adherence to established protocols, and to keep entities on track toward achieving their objectives.

Information and Communication

For an organization to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the organization to achieve all of its objectives. The information and communication Component includes the systems that support the identification, capture, and exchange of information in a form and time frame that enable personnel to carry out their responsibilities and financial reports to be generated accurately. Information and communication also spans all of the other Components of internal control.

Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on fixed assets, inventories, and receivables. Operating information is also needed to determine whether the organization is achieving its compliance requirements under various laws and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate resources[88].

[88] Adopted from the *Standards for Internal Control in the Federal Government*, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently. Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on the organization achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information[89].

Management should focus on understanding the systems and processes that are important in the accumulation of financial data, including the system of controls that safeguard information, the processes for authorizing transactions, and the system for maintaining records. When evaluating the information and communication Component of internal control over financial reporting, management should consider the methods used to accumulate and disseminate information, including:

- Accounting systems
- Policy manuals (including financial reporting manuals)
- Management's reports
- Newsletters
- Accounting policy updates
- Technical updates
- Staff meetings
- Training

When evaluating information and communication, the assessment team must consider quality, for example, ascertaining whether:

- Content is appropriate – Is the needed information available?
- Information is timely – Is it available when required?
- Information is current – Is it the latest available?
- Information is accurate – Is the data correct?
- Information is accessible – Can the data be obtained easily by appropriate parties?

All of these questions should be addressed by the system design. If not, it is probable that the system will not provide the information that management and other personnel require to ensure accurate financial reporting.

Monitoring

Monitoring is the continuous process management uses to assess the quality of internal control performance over time. There are three sub-Components to monitoring:

[89] Ibid

Figure 45: Monitoring Sub-Components

Monitoring Sub-Components	
Ongoing Monitoring	Ongoing monitoring occurs in the ordinary course of operations. Ongoing monitoring includes regular management and supervisory activities and other actions personnel take in performing duties that assess the quality of the internal control system's performance.
Separate Evaluations/ Periodic Monitoring	Periodic monitoring involves less frequent (i.e., monthly or quarterly) activities by senior management. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General.
Reporting Deficiencies	The monitoring Component should also include a process for reporting deficiencies to the appropriate level of management and undertaking remediation efforts in a timely manner.

According to the Green Book monitoring of internal control should also include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to:

- Promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations;
- Determine proper actions in response to findings and recommendations from audits and reviews; and
- Complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.

The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates the findings and recommendations do not warrant management action.

Examples of monitoring controls:

- Inspector General reviews
- Management reviews
- Self-assessments
- Reconciliations
- Fluctuation analytics
- Exception reports

The assessment team should use the DHS Entity-wide Controls Tool as a guide to document and evaluate the five internal control standards, as applicable. It will be provided as a separate attachment to this guide. The evaluation tool is based upon GAO's *Standards for Internal Control in the Federal Government* to assist agencies in maintaining or implementing effective internal controls and, when needed, to help determine what, where, and how improvements can be implemented[90]. The tool is a comprehensive questionnaire comprised of targeted questions for each factor within the five internal control standards. The assessment team should inventory existing documentation. Documentation may already exist as part of normal organizational policy or procedure; however, the assessment team should separately identify, verify, and maintain the documentation it uses in making its assessment.

The chart below, demonstrates the factors that must be documented for each Component of internal control, the level where the documentation should exist, and examples of items that may be included as part of the documentation:

Figure 46: Components of Internal Control

Internal Control Component	Factor	Level where it should be documented (Department, Organization, Locations, or Process)	Example of Items to be included in Documentation
Control Environment	▪ Integrity and Ethical Values ▪ Commitment to Competence ▪ Management's Philosophy and Operating Style ▪ Organizational Structure ▪ Assignment of Authority and Responsibility ▪ Human Resource Policies and Practices ▪ Oversight Groups	Starts at the Departmental level, but Components will need to demonstrate that the control environment operates at all levels of the organization and that they have identified their own unique organizational structure.	▪ Human Resource Policies and Procedures Manuals ▪ Organization Charts ▪ Entity Standards for Ethical Conduct ▪ Training Policies ▪ Security Handbooks ▪ Whistleblower Policies ▪ Operational Handbooks ▪ Job Descriptions including Responsibilities ▪ Relationships with Oversight Groups ▪ Related Communications at appropriate levels
Risk Assessment	▪ Establishment of Entity wide Objectives	Generally needs to be documented only at the Departmental and	▪ Policies and procedures used to identify internal and

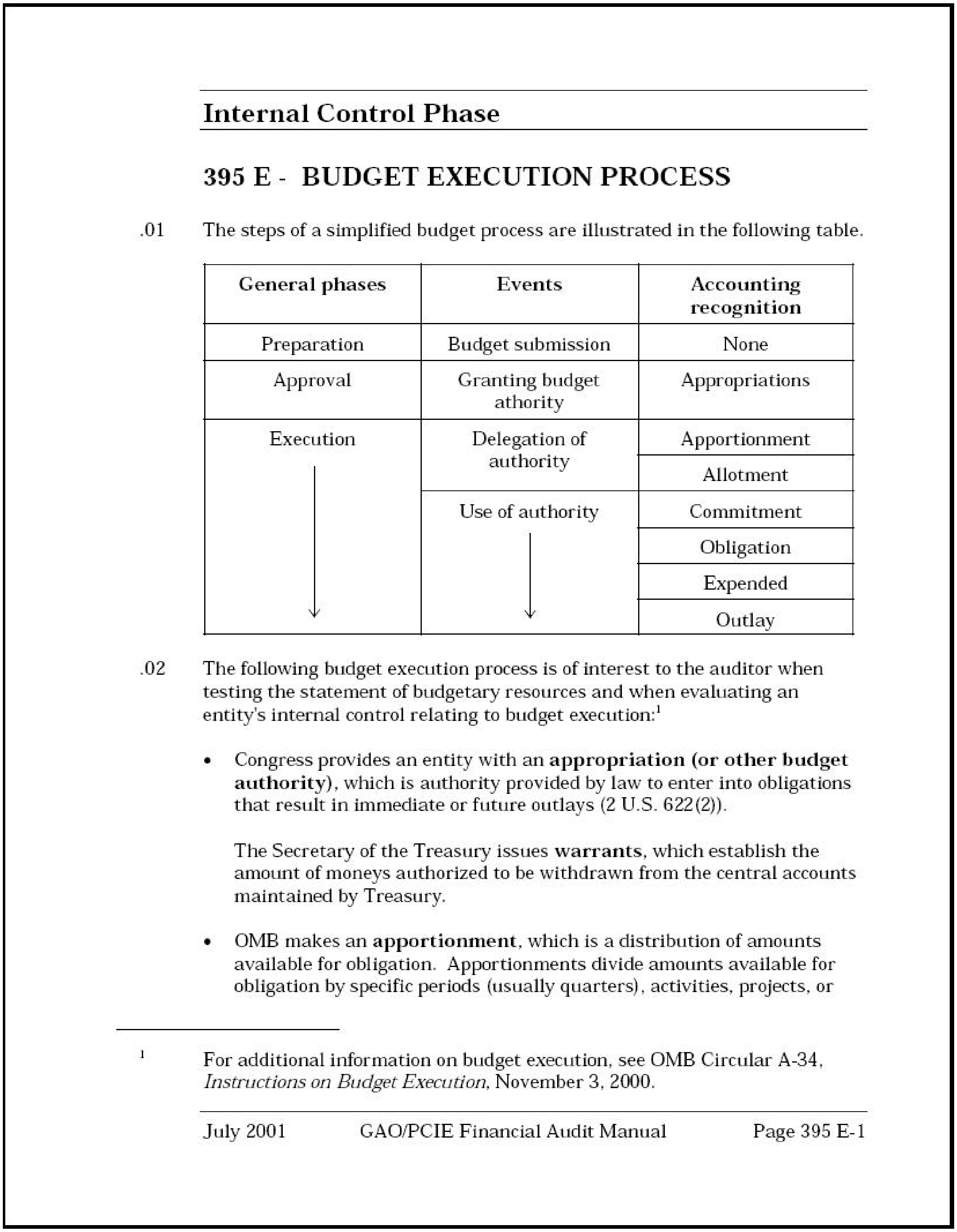
[90] GAO Report # GAO-01-1008G may be located at http://www.gao.gov/new.items/d011008g.pdf.

Internal Control Component	Factor	Level where it should be documented (Department, Organization, Locations, or Process)	Example of Items to be included in Documentation
	▪ Establishment of Activity-Level Objectives ▪ Risk Identification ▪ Risk Analysis ▪ Managing Risk Change	Component levels, unless a particular location has its own specific risk assessment process that is relevant to financial reporting.	external risks ▪ Entity Objectives and associated risks to achievement ▪ Risk Analyses and assessments ▪ Related Communications at appropriate levels
Control Activities	▪ Policies, Procedures, Techniques, and Mechanisms in place to ensure activities are properly controlled.	Generally take place at all levels, but is most commonly found at the process level. Control Activities should be documented at all levels where they exist.	▪ Management Objectives ▪ Planning and Reporting Systems ▪ Analytical Review and Analyses ▪ Policies and Procedures related to Segregation of Duties ▪ Policies and Procedures related to Safeguarding of Records ▪ Physical and Access Controls ▪ Related Communications at appropriate levels ▪ Entity-wide Security Management Program ▪ Application Controls ▪ Service Continuity ▪ Related Communications at appropriate levels
Information and Communication	▪ Process for obtaining and disseminating internal and incoming external information ▪ Process for identifying,	Starts at the Departmental level, but encompasses all levels of the organization and tends to be embedded in the other Components, particularly in the control activities Component. Therefore it should be	▪ Financial Reporting Procedures Manual ▪ Accounting Policies and Procedures ▪ Organizational Structures Indicating Lines of Communication

Internal Control Component	Factor	Level where it should be documented (Department, Organization, Locations, or Process)	Example of Items to be included in Documentation
	capturing, and distributing information ▪ Process of ensuring effective internal and external communication occurs ▪ Forms and Means of communication ▪ Disaster recovery	documented where applicable.	relevant to Financial Reporting ▪ Entity Policies Related to Distribution of Information ▪ Disaster Recovery Procedures ▪ Type and sufficiency of reports produced ▪ Communication of control related duties and responsibilities ▪ Manner in which information system development is managed ▪ Related Communications at appropriate levels
Monitoring	▪ Ongoing monitoring ▪ Separate Evaluations ▪ Reporting Deficiencies	Separate Evaluations – includes less frequent activities by senior management and can generally be documented at the entity level Ongoing Monitoring Activities – includes regular management and supervisory activities and can generally be documented with the control activities Reporting Deficiencies – includes a process for reporting internal control deficiencies to the appropriate levels of management and should be documented at the entity level	▪ Self Assessments ▪ Process for identifying the need of Self-Assessments ▪ Process for reviewing and evaluating self-assessments ▪ Process for reviewing and evaluating OIG and GAO external audit reports ▪ Process for identifying and completing and reporting corrective actions ▪ Related Communications at appropriate levels

Appendix Q – Example Walkthrough Narrative

The following walkthrough narrative is presented in order to provide a high level example of how to prepare a process narrative. The walkthrough was obtained from the GAO/PCIE Financial Audit Manual. It is not meant to be a representative example of the level of detail required for a walkthrough to be performed for the purposes of documenting controls over significant processes. Please refer to Section Four of this guide for required items that must be included in a narrative for purposes of documenting internal controls.



395 E - BUDGET EXECUTION PROCESS

.01 The steps of a simplified budget process are illustrated in the following table.

General phases	Events	Accounting recognition
Preparation	Budget submission	None
Approval	Granting budget athority	Appropriations
Execution	Delegation of authority	Apportionment
↓		Allotment
	Use of authority	Commitment
	↓	Obligation
		Expended
		Outlay

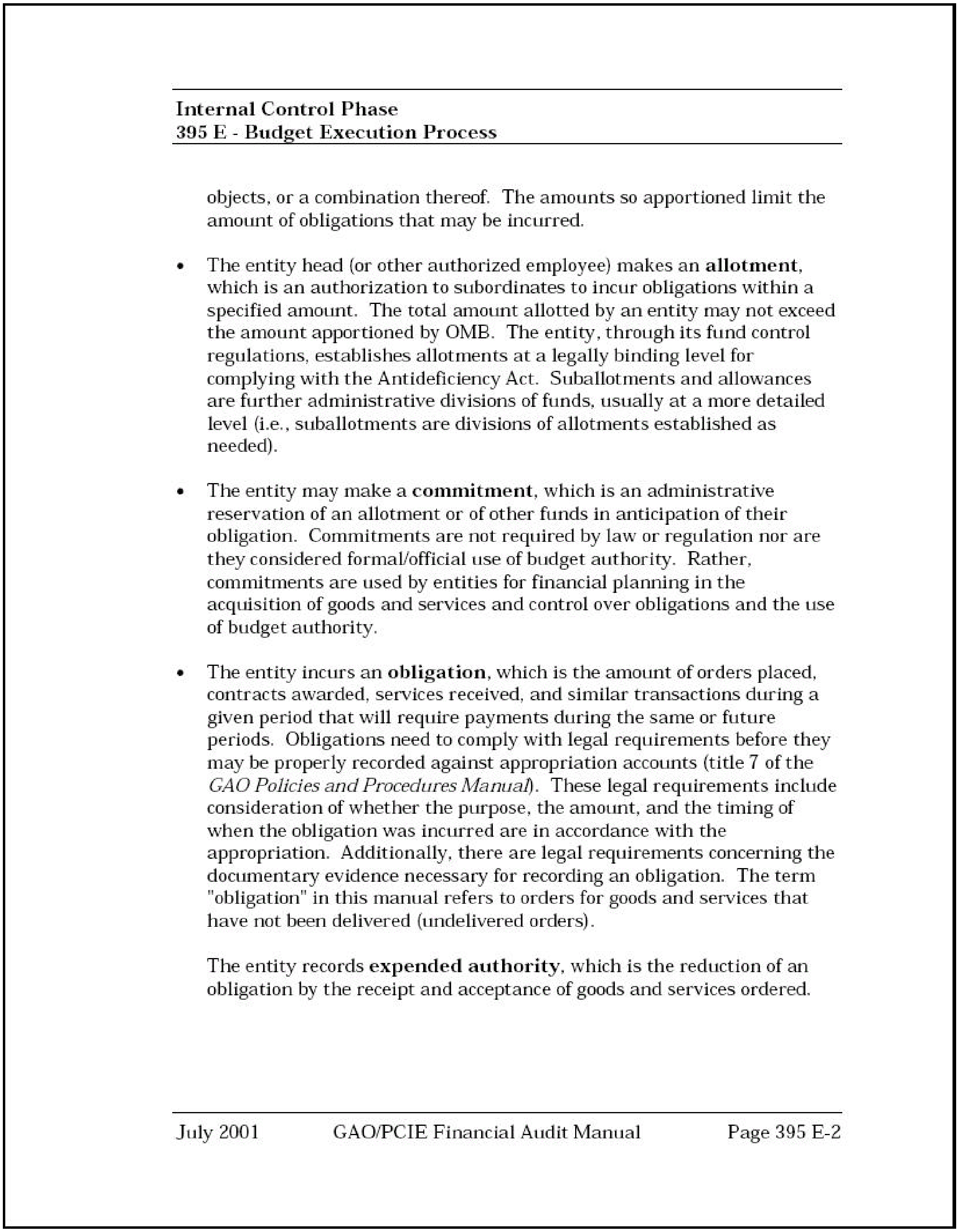
.02 The following budget execution process is of interest to the auditor when testing the statement of budgetary resources and when evaluating an entity's internal control relating to budget execution:[1]

- Congress provides an entity with an **appropriation (or other budget authority)**, which is authority provided by law to enter into obligations that result in immediate or future outlays (2 U.S. 622(2)).

  The Secretary of the Treasury issues **warrants**, which establish the amount of moneys authorized to be withdrawn from the central accounts maintained by Treasury.

- OMB makes an **apportionment**, which is a distribution of amounts available for obligation. Apportionments divide amounts available for obligation by specific periods (usually quarters), activities, projects, or

[1] For additional information on budget execution, see OMB Circular A-34, *Instructions on Budget Execution*, November 3, 2000.



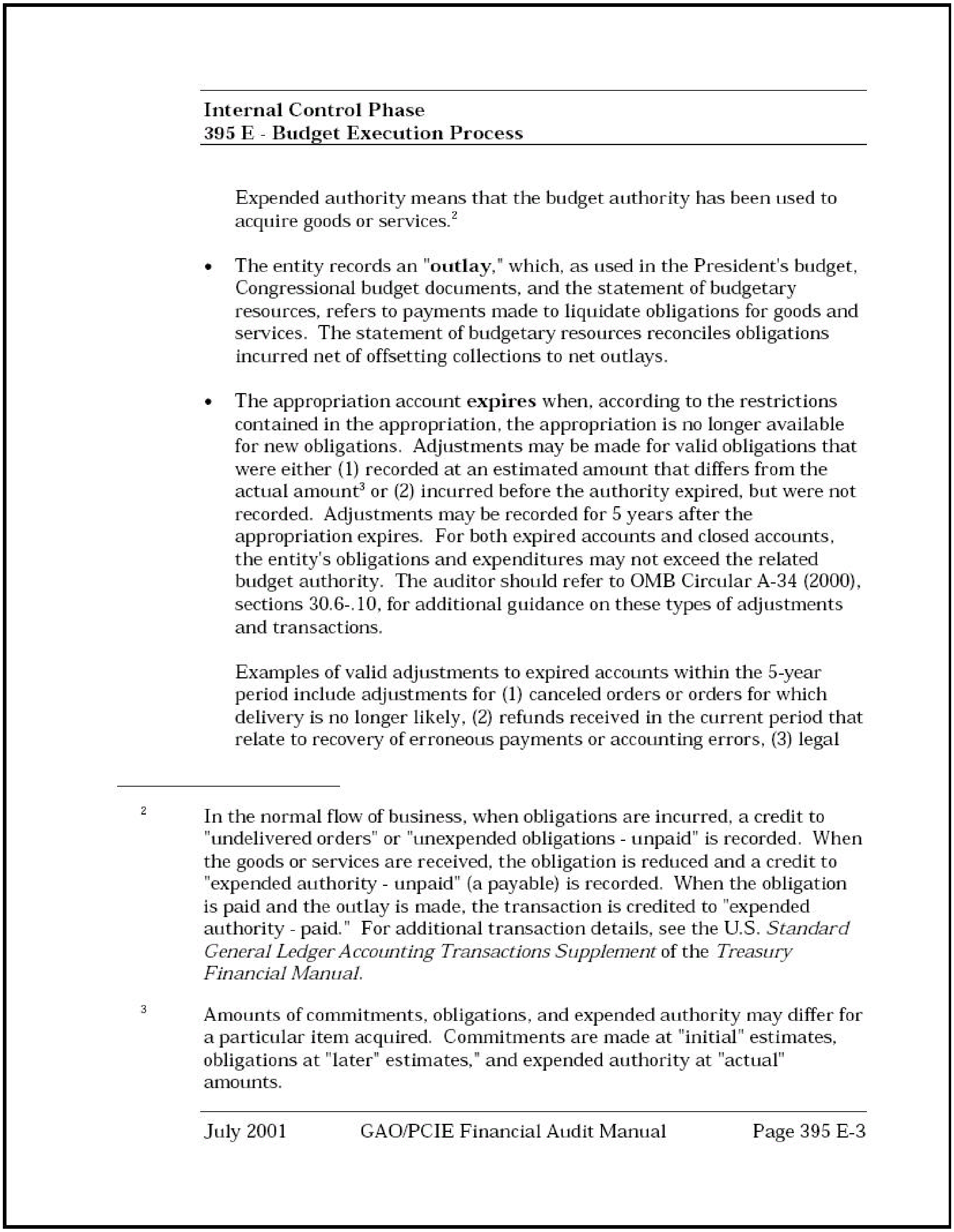
objects, or a combination thereof. The amounts so apportioned limit the amount of obligations that may be incurred.

- The entity head (or other authorized employee) makes an **allotment**, which is an authorization to subordinates to incur obligations within a specified amount. The total amount allotted by an entity may not exceed the amount apportioned by OMB. The entity, through its fund control regulations, establishes allotments at a legally binding level for complying with the Antideficiency Act. Suballotments and allowances are further administrative divisions of funds, usually at a more detailed level (i.e., suballotments are divisions of allotments established as needed).

- The entity may make a **commitment**, which is an administrative reservation of an allotment or of other funds in anticipation of their obligation. Commitments are not required by law or regulation nor are they considered formal/official use of budget authority. Rather, commitments are used by entities for financial planning in the acquisition of goods and services and control over obligations and the use of budget authority.

- The entity incurs an **obligation**, which is the amount of orders placed, contracts awarded, services received, and similar transactions during a given period that will require payments during the same or future periods. Obligations need to comply with legal requirements before they may be properly recorded against appropriation accounts (title 7 of the *GAO Policies and Procedures Manual*). These legal requirements include consideration of whether the purpose, the amount, and the timing of when the obligation was incurred are in accordance with the appropriation. Additionally, there are legal requirements concerning the documentary evidence necessary for recording an obligation. The term "obligation" in this manual refers to orders for goods and services that have not been delivered (undelivered orders).

The entity records **expended authority**, which is the reduction of an obligation by the receipt and acceptance of goods and services ordered.



Expended authority means that the budget authority has been used to acquire goods or services.[2]

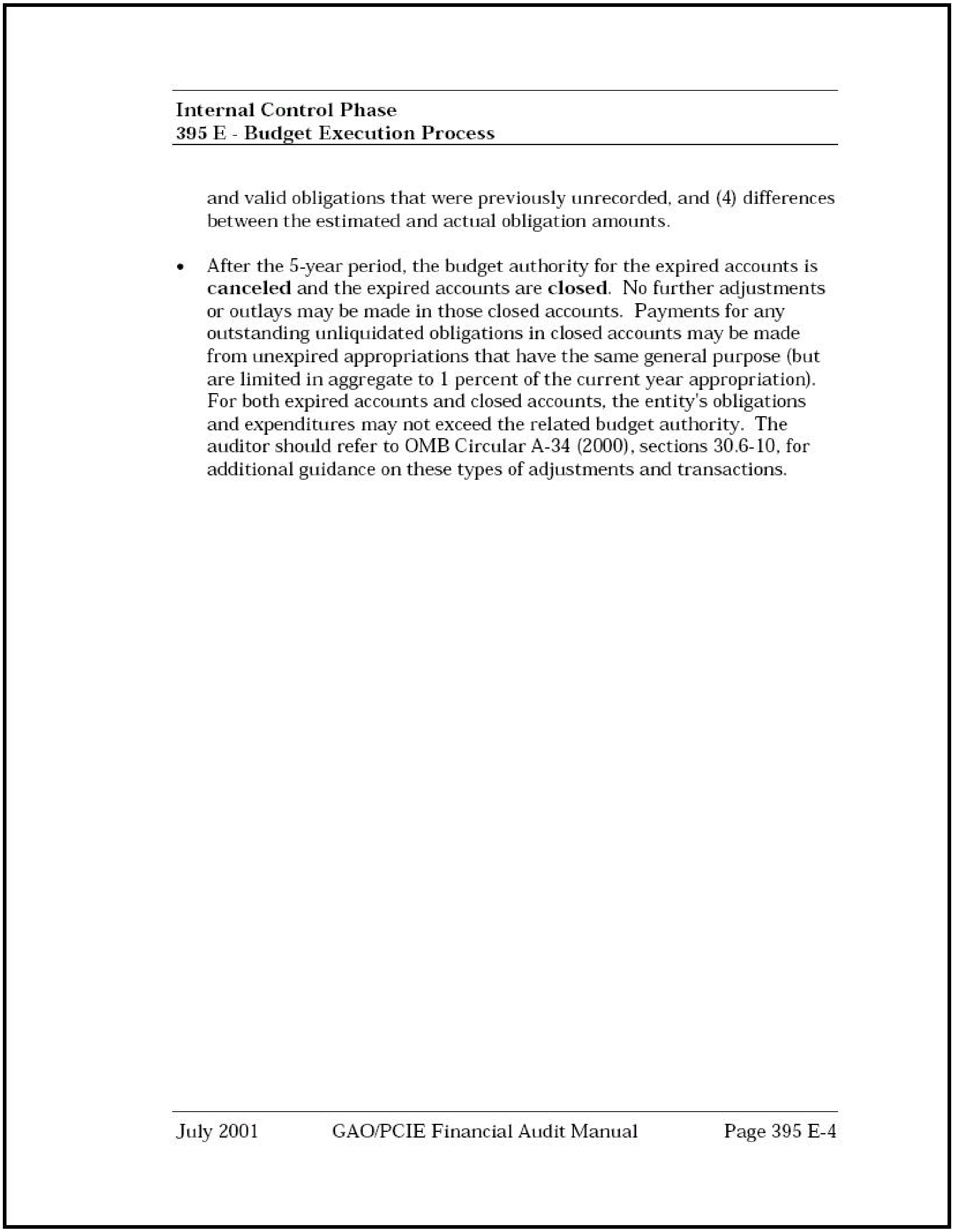
- The entity records an "**outlay**," which, as used in the President's budget, Congressional budget documents, and the statement of budgetary resources, refers to payments made to liquidate obligations for goods and services. The statement of budgetary resources reconciles obligations incurred net of offsetting collections to net outlays.

- The appropriation account **expires** when, according to the restrictions contained in the appropriation, the appropriation is no longer available for new obligations. Adjustments may be made for valid obligations that were either (1) recorded at an estimated amount that differs from the actual amount[3] or (2) incurred before the authority expired, but were not recorded. Adjustments may be recorded for 5 years after the appropriation expires. For both expired accounts and closed accounts, the entity's obligations and expenditures may not exceed the related budget authority. The auditor should refer to OMB Circular A-34 (2000), sections 30.6-.10, for additional guidance on these types of adjustments and transactions.

  Examples of valid adjustments to expired accounts within the 5-year period include adjustments for (1) canceled orders or orders for which delivery is no longer likely, (2) refunds received in the current period that relate to recovery of erroneous payments or accounting errors, (3) legal

[2] In the normal flow of business, when obligations are incurred, a credit to "undelivered orders" or "unexpended obligations - unpaid" is recorded. When the goods or services are received, the obligation is reduced and a credit to "expended authority - unpaid" (a payable) is recorded. When the obligation is paid and the outlay is made, the transaction is credited to "expended authority - paid." For additional transaction details, see the U.S. *Standard General Ledger Accounting Transactions Supplement* of the *Treasury Financial Manual.*

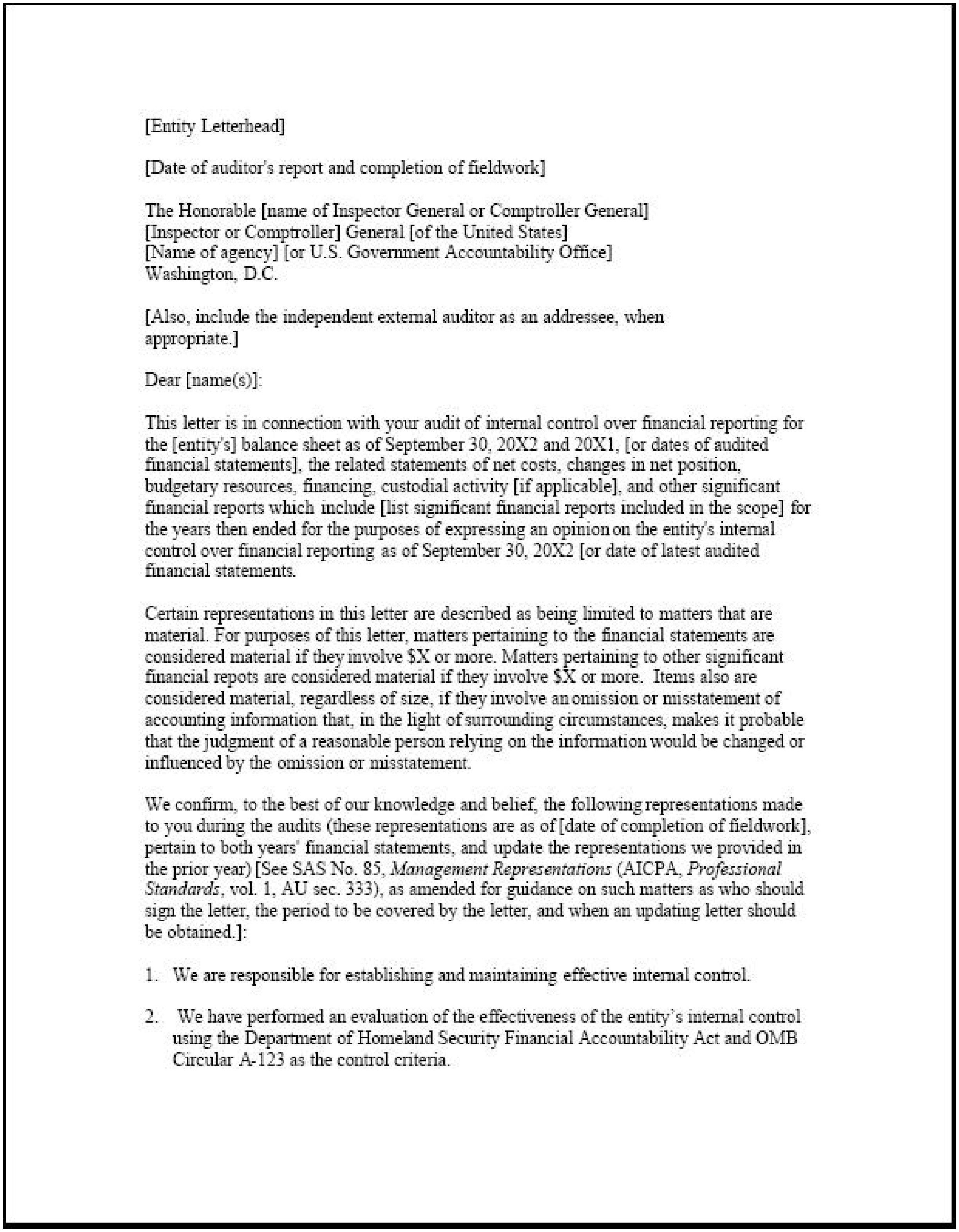
[3] Amounts of commitments, obligations, and expended authority may differ for a particular item acquired. Commitments are made at "initial" estimates, obligations at "later" estimates," and expended authority at "actual" amounts.



and valid obligations that were previously unrecorded, and (4) differences between the estimated and actual obligation amounts.

- After the 5-year period, the budget authority for the expired accounts is **canceled** and the expired accounts are **closed**. No further adjustments or outlays may be made in those closed accounts. Payments for any outstanding unliquidated obligations in closed accounts may be made from unexpired appropriations that have the same general purpose (but are limited in aggregate to 1 percent of the current year appropriation). For both expired accounts and closed accounts, the entity's obligations and expenditures may not exceed the related budget authority. The auditor should refer to OMB Circular A-34 (2000), sections 30.6-10, for additional guidance on these types of adjustments and transactions.

Appendix R – Sample Management Representation Letter



[Entity Letterhead]

[Date of auditor's report and completion of fieldwork]

The Honorable [name of Inspector General or Comptroller General]
[Inspector or Comptroller] General [of the United States]
[Name of agency] [or U.S. Government Accountability Office]
Washington, D.C.

[Also, include the independent external auditor as an addressee, when appropriate.]

Dear [name(s)]:

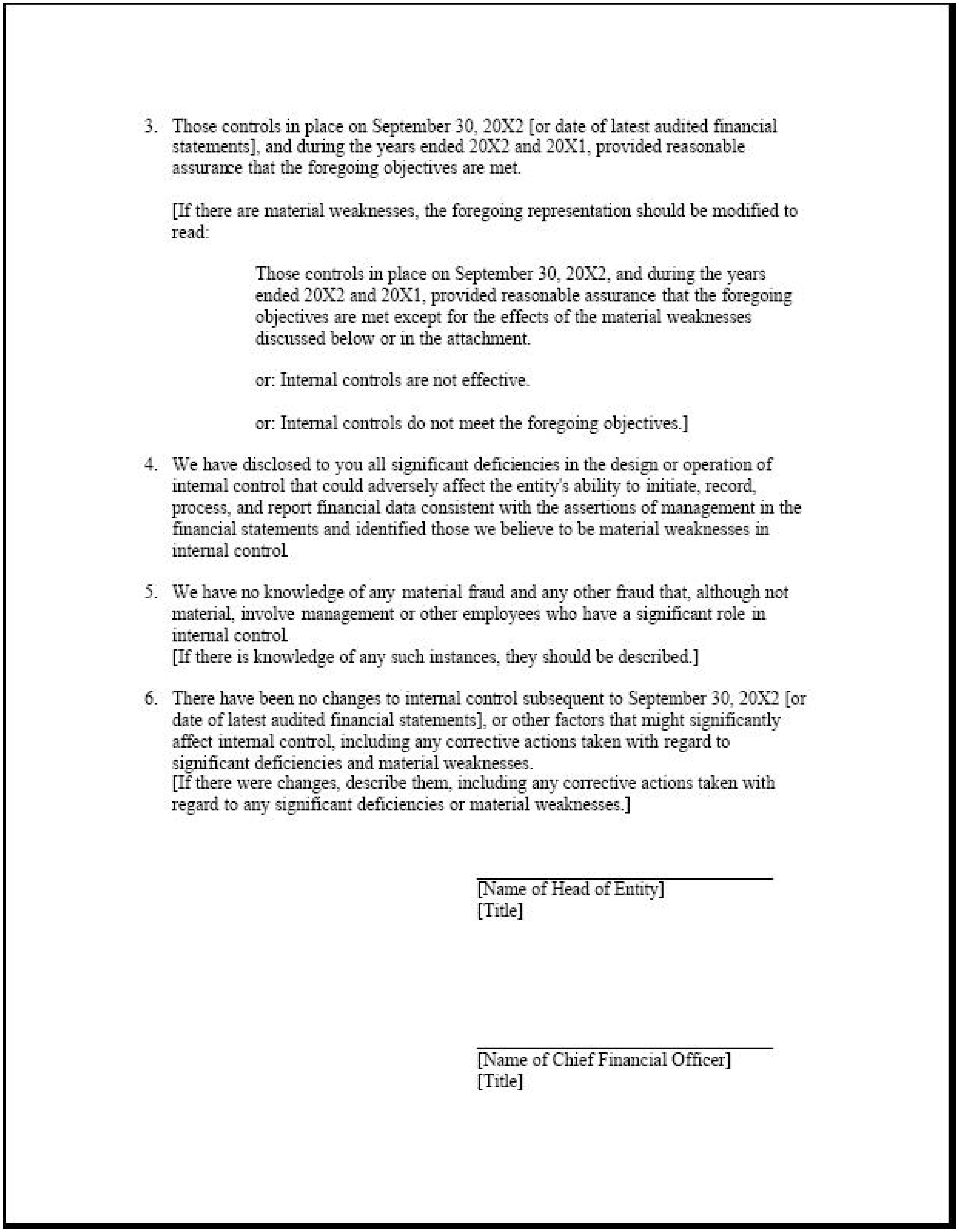
This letter is in connection with your audit of internal control over financial reporting for the [entity's] balance sheet as of September 30, 20X2 and 20X1, [or dates of audited financial statements], the related statements of net costs, changes in net position, budgetary resources, financing, custodial activity [if applicable], and other significant financial reports which include [list significant financial reports included in the scope] for the years then ended for the purposes of expressing an opinion on the entity's internal control over financial reporting as of September 30, 20X2 [or date of latest audited financial statements.

Certain representations in this letter are described as being limited to matters that are material. For purposes of this letter, matters pertaining to the financial statements are considered material if they involve $X or more. Matters pertaining to other significant financial repots are considered material if they involve $X or more. Items also are considered material, regardless of size, if they involve an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would be changed or influenced by the omission or misstatement.

We confirm, to the best of our knowledge and belief, the following representations made to you during the audits (these representations are as of [date of completion of fieldwork], pertain to both years' financial statements, and update the representations we provided in the prior year) [See SAS No. 85, *Management Representations* (AICPA, *Professional Standards*, vol. 1, AU sec. 333), as amended for guidance on such matters as who should sign the letter, the period to be covered by the letter, and when an updating letter should be obtained.]:

1. We are responsible for establishing and maintaining effective internal control.

2. We have performed an evaluation of the effectiveness of the entity's internal control using the Department of Homeland Security Financial Accountability Act and OMB Circular A-123 as the control criteria.



3. Those controls in place on September 30, 20X2 [or date of latest audited financial statements], and during the years ended 20X2 and 20X1, provided reasonable assurance that the foregoing objectives are met.

   [If there are material weaknesses, the foregoing representation should be modified to read:

   > Those controls in place on September 30, 20X2, and during the years ended 20X2 and 20X1, provided reasonable assurance that the foregoing objectives are met except for the effects of the material weaknesses discussed below or in the attachment.
   >
   > or: Internal controls are not effective.
   >
   > or: Internal controls do not meet the foregoing objectives.]

4. We have disclosed to you all significant deficiencies in the design or operation of internal control that could adversely affect the entity's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements and identified those we believe to be material weaknesses in internal control

5. We have no knowledge of any material fraud and any other fraud that, although not material, involve management or other employees who have a significant role in internal control
   [If there is knowledge of any such instances, they should be described.]

6. There have been no changes to internal control subsequent to September 30, 20X2 [or date of latest audited financial statements], or other factors that might significantly affect internal control, including any corrective actions taken with regard to significant deficiencies and material weaknesses.
   [If there were changes, describe them, including any corrective actions taken with regard to any significant deficiencies or material weaknesses.]

____
[Name of Head of Entity]
[Title]

____
[Name of Chief Financial Officer]
[Title]

Appendix S – Detail Framework for Evaluating Control Exceptions and Deficiencies[91]

The following detail framework should be used to specifically measure the magnitude and likelihood of various types of internal control deficiencies in order to determine their classification.

The evaluation of individual exceptions and deficiencies is an iterative process. Although this discussion depicts the evaluation process as a linear progression, it may be appropriate at any point in the process to return to and reconsider any previous step based on new information.

In applying the framework, the following should be considered in determining which chart(s) to use for evaluating individual exceptions and deficiencies:

- **Chart 1** is used to evaluate and **determine whether an exception** noted in performing tests of operating effectiveness **represents a control deficiency**.
- **Chart 2** is used to evaluate and classify control deficiencies in manual or automated **controls that are directly related to achieving relevant financial statement assertions**.
- **Chart 3** is used to evaluate and classify deficiencies in **general computer controls** (GCC) that are intended to support the continued effective operation of controls related to one or more relevant financial statement assertions. If an application control deficiency is related to or caused by a GCC deficiency, the application control deficiency is evaluated using Chart 2 and the GCC deficiency is evaluated using Chart 3.
- **Chart 4** is used to evaluate and classify control **deficiencies in pervasive controls other than GCC**. Such control deficiencies generally do not directly result in a misstatement. However, they may contribute to the likelihood of a misstatement at the process level.

After evaluating and classifying individual deficiencies, consideration should be given to the aggregation of the deficiencies using the guiding principles outlined in “Consider and Evaluate Deficiencies in the Aggregate” below.

Chart 1 – Evaluating Exceptions Found in the Testing of Operating Effectiveness

This decision tree is to be used for evaluating exceptions found in the testing of operating effectiveness.

General

The testing of controls generally relates to significant processes and major classes of transactions for relevant financial statement assertions related to significant accounts and disclosures. Therefore, the underlying assumption is that all exceptions/deficiencies resulting from the testing must be evaluated because they relate

[91] Adapted from A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, 12/20/2004. The framework was created by the Big 4 and other Accounting Firms and accounting educators. The whitepaper was created based off of guidance available in AS2. The framework is based on the authors’ views and is not intended to be applied universally and mechanically, but rather, with professional judgment.

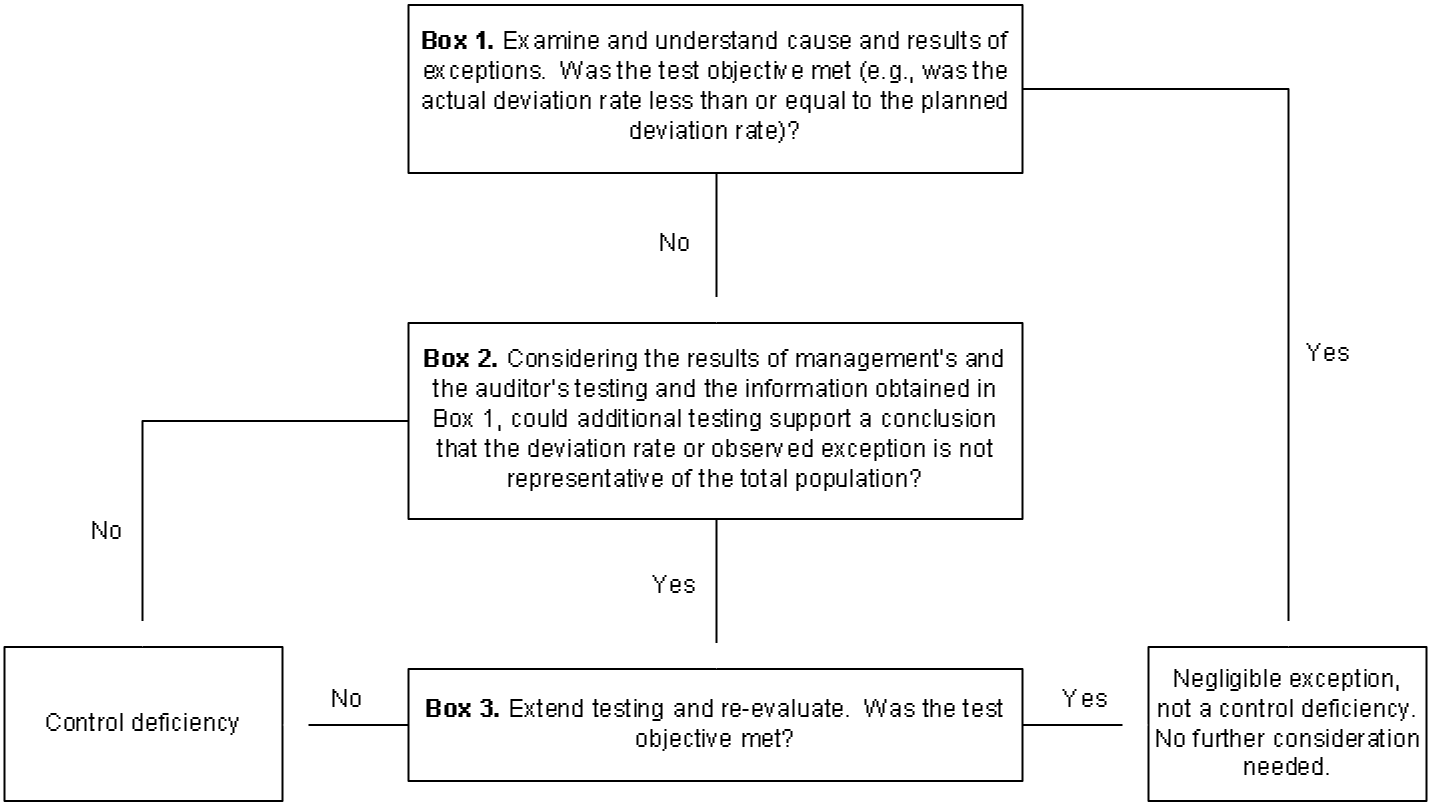
to line items, and related accounts and disclosures that are material to the financial statements taken as a whole and other significant financial reports.

The purpose of tests of controls is to achieve a high level of assurance that the controls are operating effectively. Therefore, the sample sizes used to test controls should provide that level of comfort. The sampling tables provided in this guide are based on statistical principles and generally result in a high level of assurance where no exceptions are noted. In cases in which samples are selected using a statistically based approach, sample sizes for frequently operating manual controls that result in less than a 90% level of confidence that the upper limit deviation rate does not exceed 10% typically would not provide a high level of assurance[92].

The magnitude of a control deficiency (i.e., deficiency, reportable condition, or material weakness) is evaluated based on the impact of known and/or potential misstatements on annual and interim financial statements.

While some of the concepts discussed here relate to statistical sampling, the framework does not require the use of statistical sampling. A statistical sample is (1) selected on a random or other basis that is representative of the population and (2) evaluated statistically. In tests of internal controls, it may be impractical to select samples randomly, but they should be selected in an unbiased manner.

Chart 1


Box 1. Examine and understand cause and results of exceptions. Was the test objective met (e.g., was the actual deviation rate less than or equal to the planned deviation rate)?
No
Yes
Box 2. Considering the results of management's and the auditor's testing and the information obtained in Box 1, could additional testing support a conclusion that the deviation rate or observed exception is not representative of the total population?
No
Yes
Control deficiency
No
Box 3. Extend testing and re-evaluate. Was the test objective met?
Yes
Negligible exception, not a control deficiency. No further consideration needed.

Refer to the AICPA Audit and Accounting Guide, *Audit Sampling*

Box 1

All exceptions should be evaluated quantitatively and qualitatively. A thorough understanding of the cause of the exception is important in evaluating whether a test exception represents a control deficiency. This evaluation should consider the potential implications with regard to the effectiveness of other controls.

In concluding whether the test objective was met, considerations include:

- The deviation rate in relation to the frequency of performance of the control (e.g., absent extending the test, there is a presumption that an exception in a control that operates less frequently than daily is a control deficiency).

- Qualitative factors, including exceptions that are determined to be systematic and recurring.

- Whether the exception is known to have resulted in a financial statement misstatement (e.g., there is a presumption that an exception that results in a financial statement misstatement in excess of the level of precision at which the control is designed to operate, is a control deficiency).

A control objective may be achieved by a single control or a combination of controls. A test of controls may be designed to test a single control that alone achieves the control objective or a number of individual controls that together achieve the control objective.

Box 2

If the test objective is not met, consideration should be given to whether additional testing could support a conclusion that the deviation rate is not representative of the total population. For example, if observed exceptions result in a non-negligible deviation rate, then the test objective initially is not met. In a test designed to allow for finding one or more deviations, the test objective is not met if the actual number of deviations found exceeds the number of deviations allowed for in the plan.

Box 3

If the test objective initially is not met, then there are two options:

- If the observed exceptions and resulting non-negligible deviation rate are not believed to be representative of the population, the test may be extended and re-evaluated.

- If the observed exceptions and resulting non-negligible deviation rate are believed to be representative of the population, the exceptions are considered to be a control deficiency and its significance is assessed.

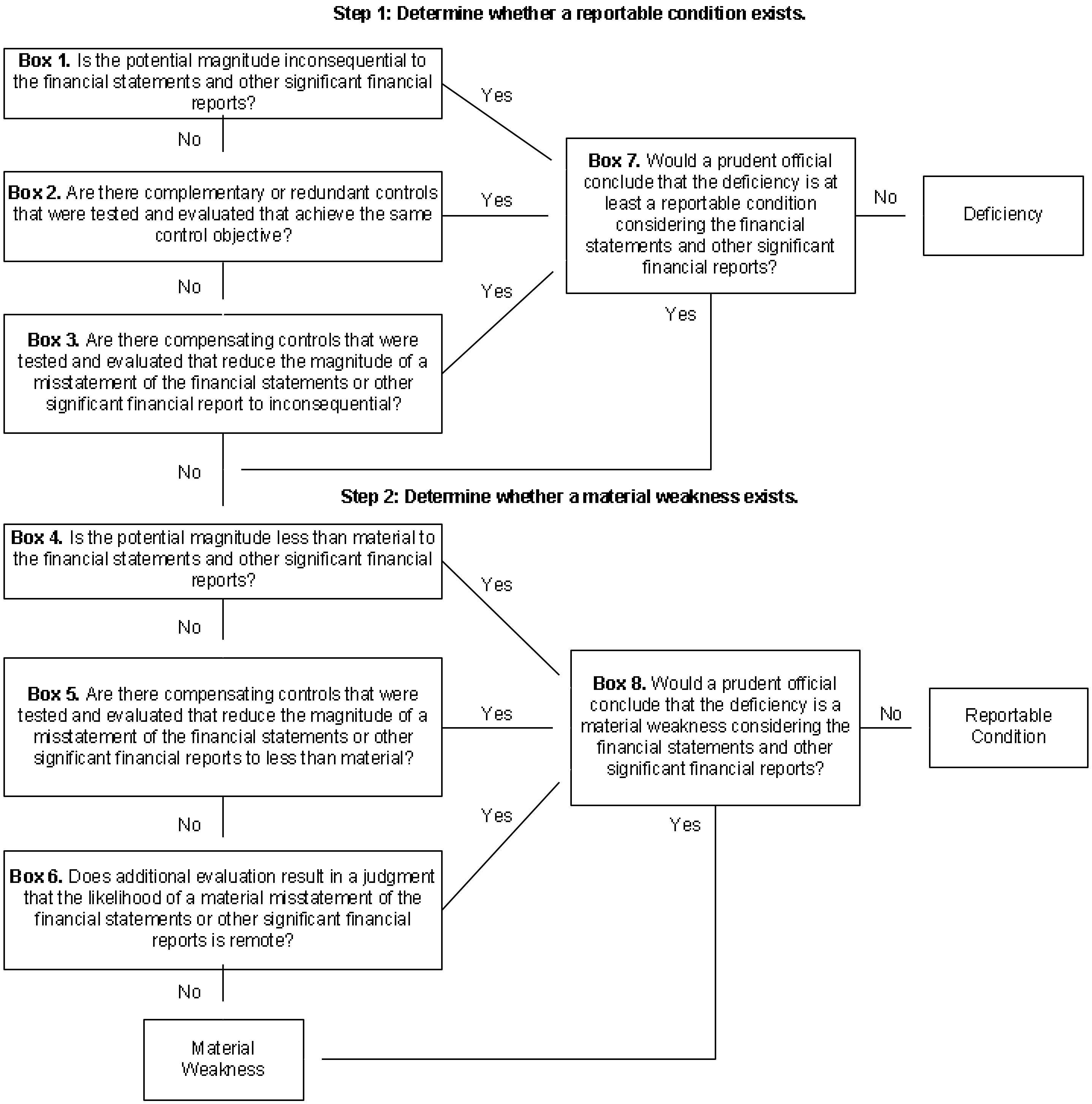
Chart 2 – Evaluating Process/Transaction-Level Control Deficiencies

This decision tree is to be used for evaluating the classification of control deficiencies from the following sources:

- Design effectiveness evaluation
- Operating effectiveness testing (from Chart 1)

- Deficiencies that resulted in a financial statement misstatement detected by management or the auditor in performing substantive test work.

Chart 2



Step 1: Determine whether a reportable condition exists.

Box 1. Is the potential magnitude inconsequential to the financial statements and other significant financial reports?

Box 2. Are there complementary or redundant controls that were tested and evaluated that achieve the same control objective?

Box 3. Are there compensating controls that were tested and evaluated that reduce the magnitude of a misstatement of the financial statements or other significant financial report to inconsequential?

Box 7. Would a prudent official conclude that the deficiency is at least a reportable condition considering the financial statements and other significant financial reports?

Deficiency

Step 2: Determine whether a material weakness exists.

Box 4. Is the potential magnitude less than material to the financial statements and other significant financial reports?

Box 5. Are there compensating controls that were tested and evaluated that reduce the magnitude of a misstatement of the financial statements or other significant financial reports to less than material?

Box 6. Does additional evaluation result in a judgment that the likelihood of a material misstatement of the financial statements or other significant financial reports is remote?

Box 8. Would a prudent official conclude that the deficiency is a material weakness considering the financial statements and other significant financial reports?

Reportable Condition

Material Weakness

Step 1. Determine whether a reportable condition exists:

Box 1

When evaluating deficiencies, potential magnitude (inconsequential, more than inconsequential, or material) is based on the potential effect on the financial statements or other significant financial reports. Potential magnitude of misstatement may be based on gross exposure, adjusted exposure, or other appropriate methods that consider the likelihood of misstatement.

Box 2 & 3

If there are controls that effectively mitigate a control deficiency, it is classified as only a deficiency, absent any qualitative factors. Such controls include:

- Complementary or redundant controls that achieve the same control objective
- Compensating controls that operate at a level of precision that would result in the prevention or detection of a *more than inconsequential* misstatement of the financial statements or other significant financial reports

Boxes 1, 2, and 3 should be considered separately. Adjusted exposure should not be reduced by the quantitative impact of the compensating and complementary or redundant controls.

Box 3

An unmitigated deficient control that results in a control objective not being met related to a significant account or disclosure generally results in a more than remote likelihood of a *more than inconsequential* misstatement of the financial statements or other significant financial reports and, therefore, is at least a reportable condition.

Step 2. Determine whether a material weakness exists:

Box 4

The potential magnitude of a misstatement of the financial statements or other significant financial report that is less than material results in the deficient control being classified as only a reportable condition, absent any qualitative factors. Potential magnitude may be based on gross exposure, adjusted exposure, or other appropriate methods that consider the likelihood of misstatement.

Box 5

Compensating controls that operate at a level of precision that would result in the prevention or detection of a *material* misstatement may support a conclusion that the deficiency is not a material weakness.

Box 6

In evaluating likelihood and magnitude, related factors include but are not limited to the following:

- The nature of the financial statement accounts, disclosures, and assertions involved; for example, suspense accounts and intraDepartmental transactions involve greater risk.
- The susceptibility of the related assets or liability to loss, waste, abuse or fraud; that is, greater susceptibility increases risk.
- The subjectivity, complexity, or extent of judgment required to determine the amount involved; that is, greater subjectivity, complexity, or judgment, like that related to an accounting estimate, increases risk.
- The cause and frequency of known or detected exceptions in the operating effectiveness of a control; for example, a control with an observed non-negligible deviation rate is a deficiency.
- The interaction or relationship with other controls; that is, the interdependence or redundancy of controls.
- The possible future consequences of the deficiency.
- An indication of increased risk evidenced by a history of misstatements, including misstatements identified in the current year.
- The adjusted exposure in relation to overall materiality.

This framework recognizes that in evaluating deficiencies, the risk of misstatement might be different for the maximum possible misstatement than for lesser possible amounts.

As a result of this additional evaluation, determine whether the likelihood of a material misstatement is remote. In extremely rare circumstances, this additional evaluation could result in a judgment that the likelihood of a more than inconsequential misstatement is remote.

Box 7 & 8

When determining the classification of a deficiency, the Senior Assessment Team should also consider the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs, such that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles[93]. If the Senior Assessment Team determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, then the auditor should deem the deficiency to be at least a reportable condition. Having determined in this manner that a deficiency represents a reportable condition, the Senior Assessment Team must further evaluate the deficiency to determine whether individually, or in combination with other deficiencies, the deficiency is a material weakness.

[93] AS 2.137

Additional considerations related to misstatements identified:

A greater than de minimis misstatement identified by the Senior Assessment Team or by the auditor during a test of controls or during a substantive test is ordinarily indicative of a deficiency in the design and/or operating effectiveness of a control, which is evaluated as follows:

- The design and/or operating deficiency(ies) that did not prevent or detect the misstatement should be identified and evaluated based on Chart 2 – Evaluating Process/Transaction-Level Control Deficiencies – applying the following:
    - A known or likely (including projected) misstatement that is inconsequential is at least a deficiency.
    - A known or likely (including projected) misstatement that is more than inconsequential is a strong indicator of a reportable condition.
    - A known or likely (including projected) misstatement that is material is at least a reportable condition and a strong indicator of a material weakness.
- The implications on the effectiveness of other controls, particularly compensating controls, also should be considered.

Chart 3 – Evaluating General Computer Control Deficiencies

This decision tree is to be used for evaluating the classification of general computer control (GCC) deficiencies from the following sources:

- GCC design effectiveness evaluation
- GCC operating effectiveness testing (from Chart 1)
- GCC design or operating deficiencies identified as a result of application control testing (from Chart 2)

General

Deficiencies in GCCs are evaluated in relation to their effect on application controls.

- GCC deficiencies do not directly result in misstatements.
- Misstatements may result from ineffective application controls.

There are three situations in which a GCC deficiency can rise to the level of a material weakness:

- An application control deficiency related to or caused by a GCC deficiency is classified as a material weakness
- The pervasiveness and significance of a GCC deficiency leads to a conclusion that there is a material weakness in the entity's control environment

- A GCC deficiency classified as a reportable condition remains uncorrected after some reasonable period of time

In evaluating whether a GCC deficiency effects the continued effective operation of application controls, it is not necessary to contemplate the likelihood that an effective application control could, in a subsequent year, become ineffective because of the deficient GCC.

Relationship between GCCs and application controls.

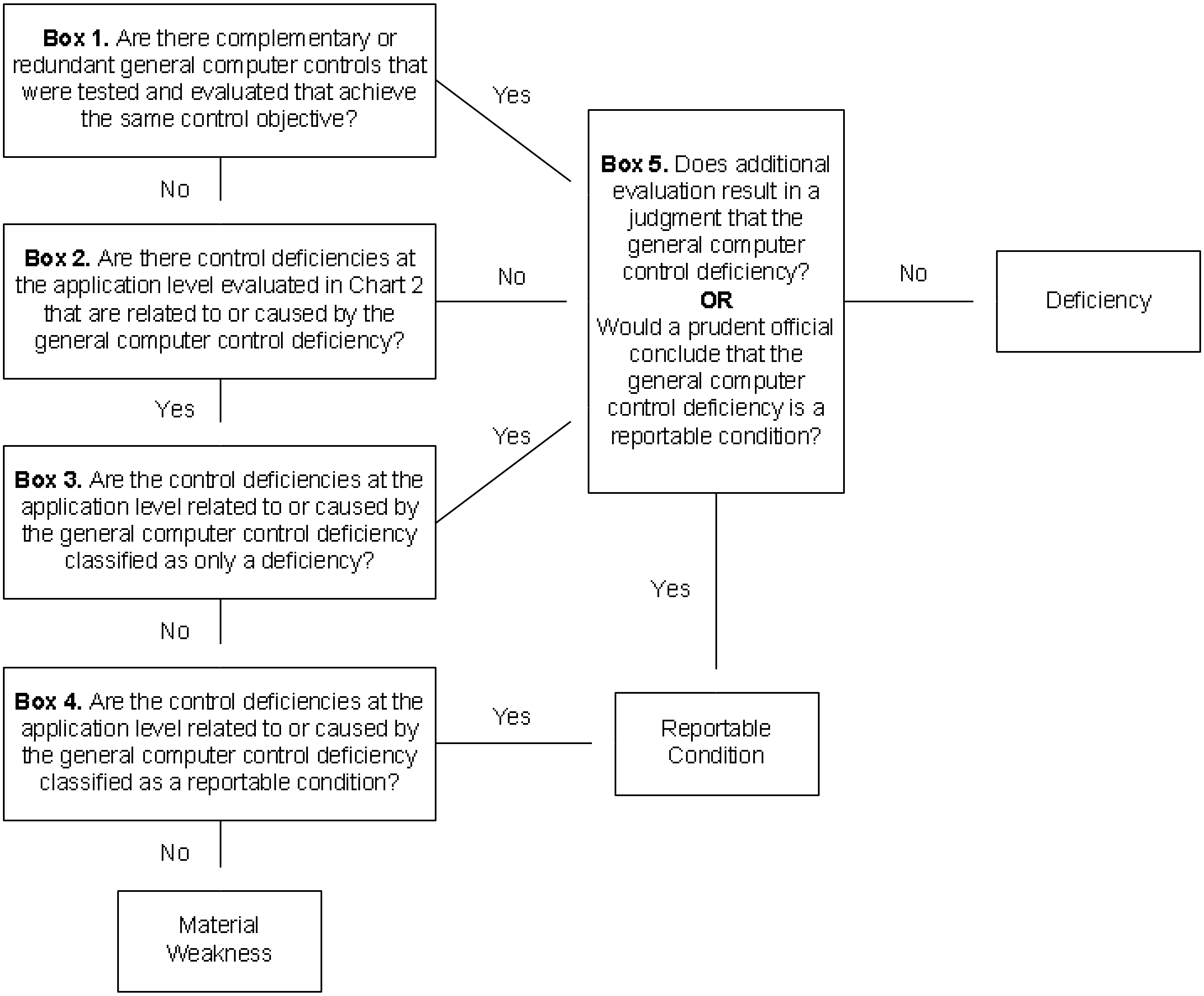
An understanding of the relationship among applications relevant to internal control over financial reporting, the related application controls, and GCCs is necessary to appropriately evaluate GCC deficiencies. GCCs may affect the continued effective operation of application controls. For example, an effective security administration function supports the continued effective functioning of application controls that restrict access. As another example, effective program change controls support the continued effective operation of programmed application controls, such as a three-way match. GCCs also may serve as controls at the application level. For example, GCCs may directly achieve the control objective of restricting access and thereby prevent initiation of unauthorized transactions.

Similarly, GCC deficiencies may adversely affect the continued effective functioning of application controls; in the absence of application controls, GCC deficiencies also may represent control deficiencies for one or more relevant assertions.

Evaluating GCC deficiencies.

All GCC deficiencies are evaluated using Chart 3. Additionally, if a GCC deficiency also represents a deficiency at the application level because it directly relates to an assertion, the GCC deficiency is also evaluated using Chart 2. In all cases, a GCC deficiency is considered in combination with application controls to determine whether the combined effect of the GCC deficiency and any application control deficiencies is a deficiency, reportable condition, or material weakness.

Chart 3


Box 1. Are there complementary or redundant general computer controls that were tested and evaluated that achieve the same control objective?
Yes
No
Box 2. Are there control deficiencies at the application level evaluated in Chart 2 that are related to or caused by the general computer control deficiency?
No
Yes
Box 3. Are the control deficiencies at the application level related to or caused by the general computer control deficiency classified as only a deficiency?
Yes
No
Box 4. Are the control deficiencies at the application level related to or caused by the general computer control deficiency classified as a reportable condition?
Yes
No
Material Weakness
Box 5. Does additional evaluation result in a judgment that the general computer control deficiency? OR Would a prudent official conclude that the general computer control deficiency is a reportable condition?
No
Deficiency
Yes
Reportable Condition

Box 2

If no deficiencies are identified at the application level (as evaluated in Chart 2), the GCC deficiency could be classified as only a deficiency. (Refer to Box 5.)

Box 3 & 4

If there is a control deficiency at the application level related to or caused by a GCC deficiency, the GCC deficiency is evaluated in combination with the deficiency in the underlying application control and generally is classified consistent with the application control deficiency. As a result:

- A material weakness in an application control related to or caused by a GCC deficiency indicates that the GCC deficiency also is a material weakness.
- A reportable condition in an application control related to or caused by a GCC deficiency indicates that the GCC deficiency also is a reportable condition.
- An application control deficiency (that is only a deficiency) related to or caused by a GCC deficiency generally indicates that the GCC deficiency is only a deficiency.

Box 5

Notwithstanding the guiding principles relating to Boxes 1 through 4, the classification of a GCC deficiency should consider factors including, but not limited to, the following:

- The nature and significance of the deficiency, e.g., does the deficiency relate to a single area in the program development process or is the entire process deficient?
- The pervasiveness of the deficiency to applications and data, including:
  - The extent to which controls related to significant accounts and underlying processes are affected by the deficiency
  - The number of application controls that are related to the deficiency
  - The number of control deficiencies at the application level that are related to or caused by the deficiency
- The complexity of the entity’s systems environment and the likelihood that the deficiency could adversely affect application controls
- The relative proximity of the control to applications and data
- Whether a deficiency relates to applications or data for accounts or disclosures that are susceptible to loss or fraud
- The cause and frequency of known or detected exceptions in the operating effectiveness of a GCC; for example, (1) a control with an observed non-negligible deviation rate, (2) an observed exception that is inconsistent with the expected effective operation of the GCC, or (3) a deliberate failure to apply a control .
- An indication of increased risk evidenced by a history of misstatements relating to applications affected by the deficiency, including misstatements in the current year

When determining the classification of a deficiency, the Senior Assessment Team should determine the level of detail and degree of assurance that would satisfy prudent officials[94] in the conduct of their own affairs. The Senior Assessment Team then can have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles. If the Senior Assessment Team determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, then deficiency should be deemed to be at least a reportable condition.

Additional consideration:

GCCs support the proper and consistent operation of automated application controls. Therefore, consideration should be given to the nature, timing, and extent of the testing of related application controls affected by, or manual controls dependent on, the deficient GCC.

Chart 4 – Evaluating Control Deficiencies in Pervasive Controls Other than GCC

This decision tree is to be used for evaluating the classification of control deficiencies in pervasive controls other than GCC from the following sources:

- Design effectiveness evaluation
- Operating effectiveness testing (from Chart 1)

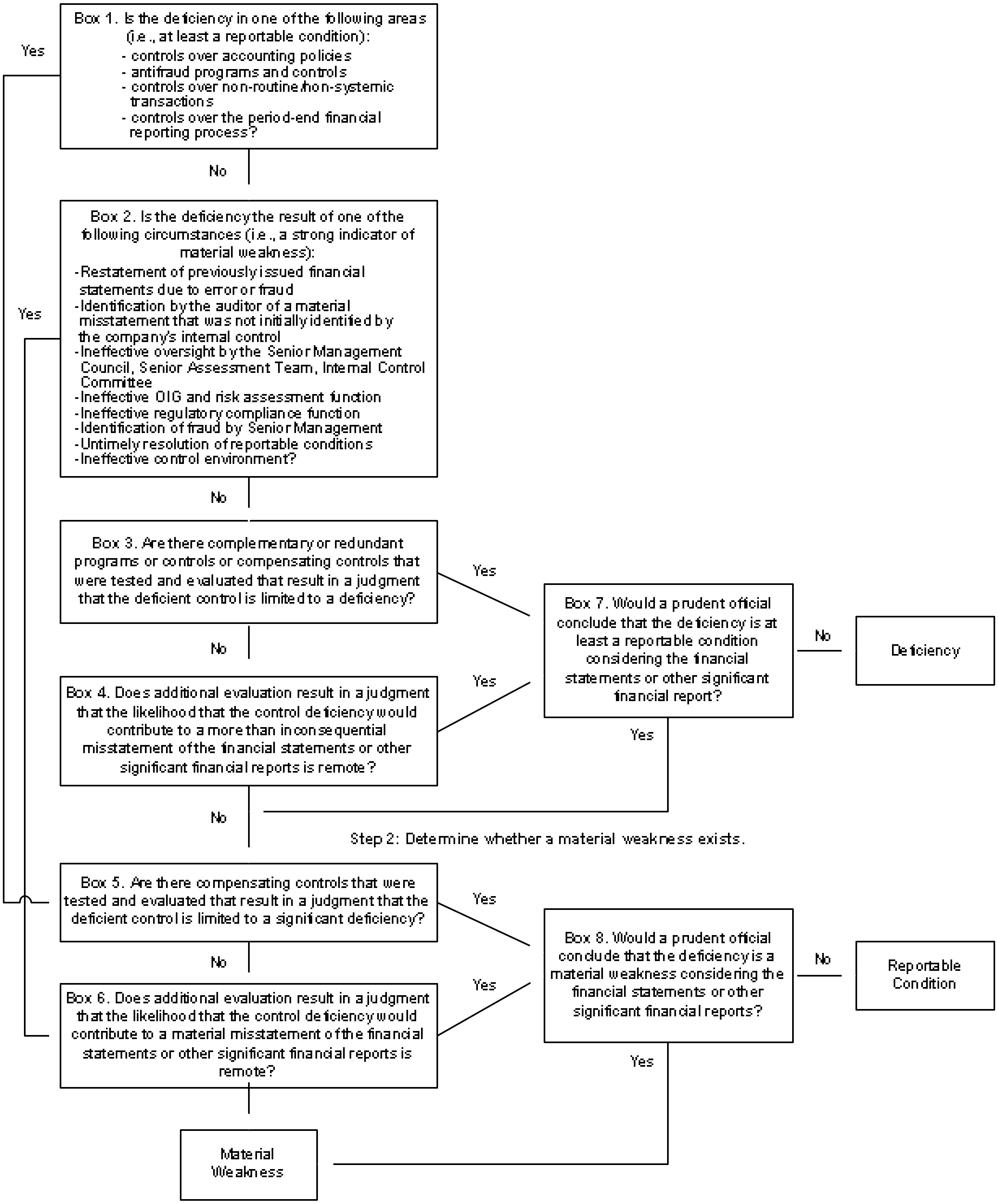
General

Deficiencies in pervasive controls generally do not directly result in a misstatement. However, they may contribute to the likelihood of a misstatement at the process level. Accordingly, evaluation of a deficiency in a pervasive control other than GCC is based on the likelihood that such deficiency would contribute to circumstances that could result in a misstatement. Quantitative methods generally are not conducive to evaluating such deficiencies.

[94] The idea of "prudent official" and related discussion is based off of AS 2.137.

Chart 4

Step 1: Determine whether a reportable condition exists.


Box 1. Is the deficiency in one of the following areas (i.e., at least a reportable condition):
- controls over accounting policies
- antifraud programs and controls
- controls over non-routine/non-systemic transactions
- controls over the period-end financial reporting process?
Yes
No
Box 2. Is the deficiency the result of one of the following circumstances (i.e., a strong indicator of material weakness):
-Restatement of previously issued financial statements due to error or fraud
-Identification by the auditor of a material misstatement that was not initially identified by the company's internal control
-Ineffective oversight by the Senior Management Council, Senior Assessment Team, Internal Control Committee
-Ineffective OIG and risk assessment function
-Ineffective regulatory compliance function
-Identification of fraud by Senior Management
-Untimely resolution of reportable conditions
-Ineffective control environment?
Yes
No
Box 3. Are there complementary or redundant programs or controls or compensating controls that were tested and evaluated that result in a judgment that the deficient control is limited to a deficiency?
Yes
No
Box 4. Does additional evaluation result in a judgment that the likelihood that the control deficiency would contribute to a more than inconsequential misstatement of the financial statements or other significant financial reports is remote?
Yes
No
Box 7. Would a prudent official conclude that the deficiency is at least a reportable condition considering the financial statements or other significant financial report?
No
Deficiency
Yes
Step 2: Determine whether a material weakness exists.
Box 5. Are there compensating controls that were tested and evaluated that result in a judgment that the deficient control is limited to a significant deficiency?
Yes
No
Box 6. Does additional evaluation result in a judgment that the likelihood that the control deficiency would contribute to a material misstatement of the financial statements or other significant financial reports is remote?
Yes
Box 8. Would a prudent official conclude that the deficiency is a material weakness considering the financial statements or other significant financial reports?
No
Reportable Condition
Yes
Material Weakness

Step 1. Determine whether a reportable condition exists:

Box 1 & 2

A deficiency in one of the following areas ordinarily results in deficiencies being at least a reportable condition[95]:

- Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles;
- Anti-fraud programs and controls;
- Controls over non-routine and non-systematic transactions; and
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; initiate, authorize, record, and process journal entries into the general ledger; and record the recurring and nonrecurring adjustments to the financial statements.

The circumstances in which an evaluation would lead to the deficiency not being classified as a reportable condition are rare. The following circumstances should be regarded as at least a reportable condition and as a strong indicator of a material weakness[96]:

- Restatement of previously issued financial statements due to error or fraud to reflect the correction of a misstatement.
- Identification by the auditor of a material misstatement in financial statements in the current period that was not initially identified by the entity's internal control over financial reporting. This is a strong indicator of a material weakness even if management subsequently corrects the misstatement.
- Oversight of the external financial reporting and internal control over financial reporting by the Senior Management Council, Senior Assessment Team, or Internal Control Committee is ineffective.
- The OIG function or the risk assessment function is ineffective in the monitoring Component or risk assessment Component.
- An ineffective regulatory compliance function that is solely related to those aspects of ineffective regulatory compliance in which associated violations of laws and regulations could have a material effect on the reliability of financial reporting.
- Identification of fraud of any magnitude on the part of senior management.

[95] Based on guidance provided in AS 2.139.

[96] Based on guidance provided in AS 2.140.

- Reportable Conditions that have been communicated to the Senior Management Council and Senior Assessment Team remain uncorrected after a reasonable period of time.
- An ineffective control environment.

Box 3

Certain controls could result in a judgment that the deficient control is limited to a deficiency and classified as only a deficiency, considering qualitative factors. Such controls include:

- Complementary or redundant programs or controls
- Compensating controls within the same or another Component

Box 4

A deficiency with a more than remote likelihood that the deficiency would contribute to a more than inconsequential misstatement is a reportable condition. Such judgment considers an evaluation of factors such as:

- The pervasiveness of the deficiency across the entity
- The relative significance of the deficient control to the location
- An indication of increased risks of error (evidenced by a history of misstatement)
- An increased susceptibility to fraud (including the risk of management override)
- The cause and frequency of known or detected exceptions for the operating effectiveness of a control
- The possible future consequences of the deficiency

Step 2. Determine whether a material weakness exists:

Box 5

The evaluation of certain controls could result in a judgment that the deficient control is limited to a reportable condition and classified as such, considering qualitative factors. Such controls include compensating controls within the same or another Component.

Box 6

A deficiency with a more than remote likelihood that the deficiency would contribute to a material misstatement is a material weakness. Such judgment considers an evaluation of factors such as:

- The pervasiveness of the deficiency across the entity
- The relative significance of the deficient control to the location
- An indication of increased risks of error (evidenced by a history of misstatement)

- An increased susceptibility to fraud (including the risk of management override)
- The cause and frequency of known or detected exceptions for the operating effectiveness of a control
- The possible future consequences of the deficiency

A deficiency of the type described in **Box 2** is generally a material weakness; in limited circumstances, it may be appropriate to conclude the deficiency is only a reportable condition. The only circumstance that would likely occur is[97]:

- The auditor initially identified a material misstatement in the financial statements but, given the circumstances, determined that management ultimately would have found the misstatement, the auditor could determine that the circumstance was a reportable condition, but not a material weakness.

In this case, the deficiency would be a reportable condition.

Box 7 & 8

When determining the classification of a deficiency in internal control over financial reporting, the Senior Assessment Team should also consider, the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs, such that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles[98]. If the Senior Assessment Team determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, then the Senior Assessment Team should deem the deficiency to be at least a reportable condition. Having determined in this manner that a deficiency represents a reportable condition, the Senior Assessment Team must further evaluate the deficiency to determine whether individually, or in combination with other deficiencies, the deficiency is a material weakness.

Consider and Evaluate Deficiencies in the Aggregate

Deficiencies are considered in the aggregate by significant account balance, disclosure and Internal Control Standards Component to determine whether they collectively result in reportable conditions or material weaknesses. Aggregation of control activities deficiencies by significant account balance and disclosure is necessary since the existence of multiple control deficiencies related to a specific account balance or disclosure increases the likelihood of misstatement. Aggregation by the control environment, risk assessment, information and communication, and monitoring Components of Internal Control Standards is more difficult and judgmental. For example, unrelated control deficiencies relating to design ineffectiveness in other Internal Control Standards Components could lead to the conclusion that a reportable condition or material weakness in the risk assessment Component exists. Similarly, unrelated control deficiencies in other Internal Control Standards Components could lead to a conclusion that a reportable condition or material weakness in the control environment or monitoring Component exists.

[97] Based on guidance provided in AS2 Appendix E99.

[98] AS 2.137

Appendix T – Summary of Aggregated Differences (SAD)

Schedule of Aggregated Control Deficiencies

The Summary of Aggregated Deficiencies (SACD) is a tool to assist the Assessment Team, OFM, and the ICC Board in:

- evaluating the significance of internal control deficiencies, individually and in the aggregate;
- identifying themes and trends common to two or more deficiencies.

This template enables the Assessment Team to sort internal control deficiencies by Component, process, the GAO standard for internal control, financial statement assertion, and account, class of transactions and type of disclosure.

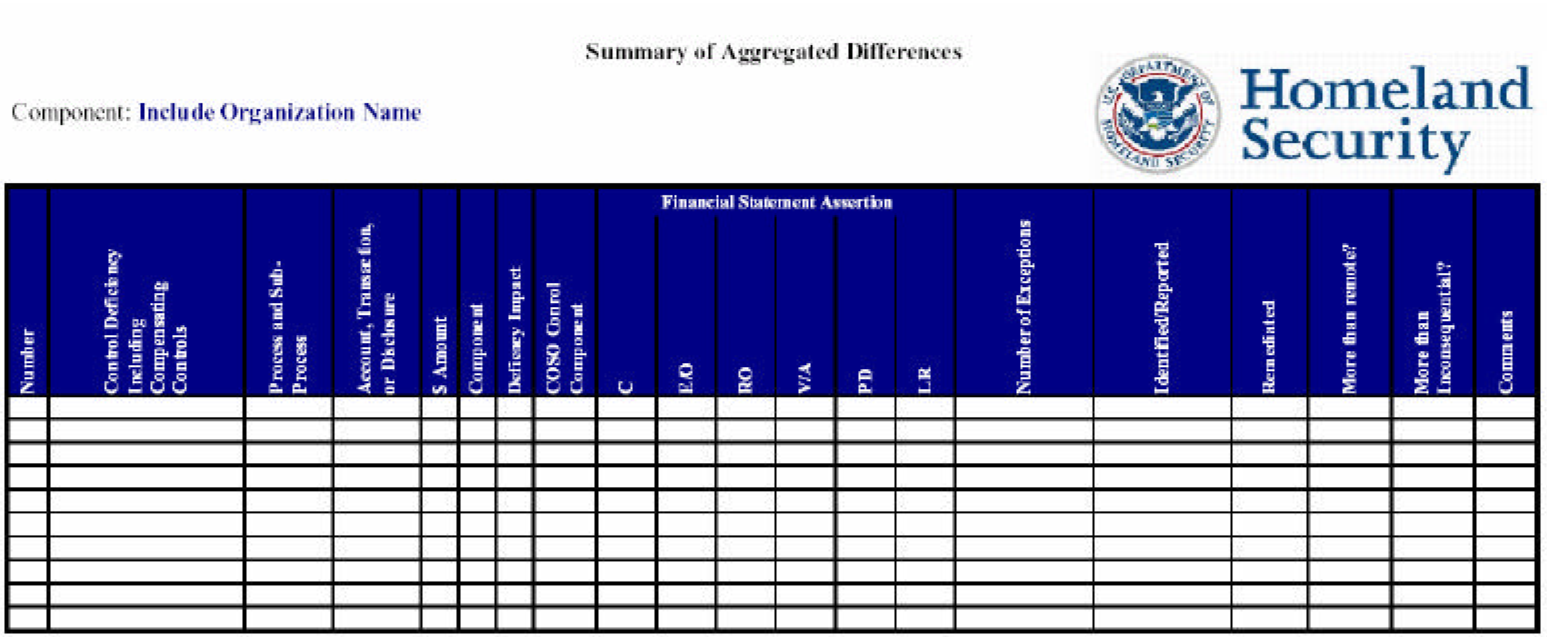
All internal control deficiencies should be posted to the SACD during the course of the project, including deficiencies identified by management and others. Internal control deficiencies posted to the SACD should be communicated and discussed with the Assessment Team Lead, and Component CFO and CIO timely.

Column	**Explanation**
Number	Allows for identification of internal control deficiencies
Control Deficiency, including compensating controls	Description of internal control deficiency and description of other controls or circumstances that either reduce the likelihood of the deficiency or the exposure of the deficiency (i.e., mitigating control).
Process and Sub-Process	Process and sub-process affected by the internal control deficiency.
Account, Transaction or Disclosure	Accounts, transactions and disclosures related to the internal control deficiency. Note: (1) be as descriptive of the account as possible (i.e., “earned revenue” instead of “revenue”) and (2) most deficiencies will affect several accounts, transactions and disclosures; however, due to the limitations in Excel, the deficiency should be repeated on a separate line for each account, transaction or disclosure it affects.
$ Amount	Represents the actual dollar amount of a misstatement if one occurred or projected impact, if measurable (for example, balance of receivables over days).
Component	Component in which the internal control deficiency arose.
Deficiency Impact	Designation of whether the internal control deficiency is a deficiency in design of system or operating effectiveness or both.
GAO Standards for Internal Control	Federal Government Standard for Internal Control Component affected by internal control deficiency (i.e., Control Environment, Risk Assessment, Monitoring of Controls, Information & Communication, Control Activities). Note: Many deficiencies will affect several control Components. Use this column to indicate the most relevant control Component and indicate other control Components affected in the “Comments” box.

Schedule of Aggregated Control Deficiencies

Financial Statement Assertion	Indicate which of the financial statement assertions are affected by the internal control deficiency
No. of Exceptions	Number of exceptions which occurred if the internal control deficiency was an operating deficiency
Identification/Reported	Indicate whether the deficiency was identified by management but not reported, identified by management and reported, or identified by the auditor
Remediation	Has the deficiency been remediated?
More than remote?	Is the likelihood that the internal control deficiency could result in a misstatement of an account or disclosure more than remote, after considering mitigating controls?
More than inconsequential?	Is the potential magnitude of the impact of the internal control deficiency on the financial statements more than inconsequential, after considering mitigating controls?
Comments	Other relevant information necessary for explanatory purposes.

Figure 47: Summary of Aggregated Differences

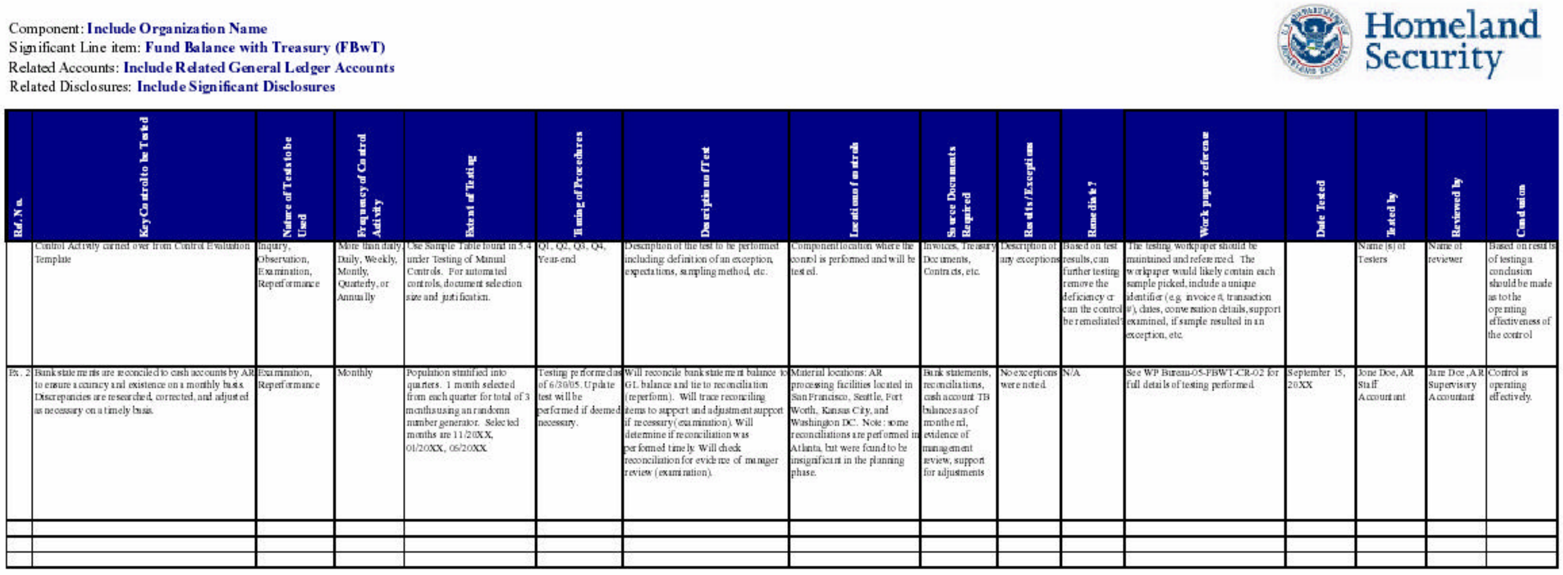


Summary of Aggregated Differences

Component: Include Organization Name

Number	Control Deficiency Including Compensating Controls	Process and Sub-Process	Account, Transaction, or Disclosure	$ Amount	Component	Defiency Impact	COSO Conrol Component	Financial Statement Assertion						Number of Exceptions	Identified/Reported	Remediated	More than remote?	More than Inconsequential?	Comments
								C	E/O	RO	V/A	PD	LR						

Appendix U – Testing Plan Template



Component: **Include Organization Name**
Significant Line item: **Fund Balance with Treasury (FBwT)**
Related Accounts: **Include Related General Ledger Accounts**
Related Disclosures: **Include Significant Disclosures**

Ref. No.	Key Controls to be Tested	Nature of Tests to be Used	Frequency of Control Activity	Extent of Testing	Timing of Procedures	Description of Test	Locations of controls	Source Documents Required	Results/Exceptions	Remediate?	Work paper reference	Date Tested	Tested by	Reviewed by	Conclusion
	Control Activity carried over from Control Evaluation Template	Inquiry, Observation, Examination, Reperformance	More than daily, Daily, Weekly, Montly, Quarterly, or Annually	Use Sample Table found in 5.4 under Testing of Manual Controls. For automated controls, document selection size and justification.	Q1, Q2, Q3, Q4, Year-end	Description of the test to be performed including definition of an exception, expectations, sampling method, etc.	Component location where the control is performed and will be tested.	Invoices, Treasury Documents, Contracts, etc.	Description of any exceptions	Based on test results, can further testing remove the deficiency or can the control be remediated?	The testing workpaper should be maintained and referenced. The workpaper would likely contain each sample picked, include a unique identifier (e.g. invoice #, transaction #), dates, conversation details, support examined, if sample resulted in an exception, etc.		Name (s) of Testers	Name of reviewer	Based on results of testing a conclusion should be made as to the operating effectiveness of the control
Ex. 2	Bank statements are reconciled to cash accounts by AR to ensure accuracy and existence on a monthly basis. Discrepancies are researched, corrected, and adjusted as necessary on a timely basis.	Examination, Reperformance	Monthly	Population stratified into quarters. 1 month selected from each quarter for total of 3 months using an random number generator. Selected months are 11/20XX, 01/20XX, 06/20XX.	Testing performed as of 6/30/05. Update test will be performed if deemed necessary.	Will reconcile bank statement balance to GL balance and tie to reconciliation (reperform). Will trace reconciling items to support and adjustment support if necessary (examination). Will determine if reconciliation was performed timely. Will check reconciliation for evidence of manager review (examination).	Material locations: AR processing facilities located in San Francisco, Seattle, Fort Worth, Kansas City, and Washington DC. Note: some reconciliations are performed in Atlanta, but were found to be insignificant in the planning phase.	Bank statements, reconciliations, cash account TB balances as of month end, evidence of management review, support for adjustments	No exceptions were noted.	N/A	See WP Bureau-05-FBWT-CR-02 for full details of testing performed.	September 15, 20XX	Jone Doe, AR Staff Accountant	Jane Doe, AR Supervisory Accountant	Control is operating effectively.

Homeland Security

Special thanks to the Department's professionals listed below that made significant contributions to our initial steps in responding to the Department of Homeland Security Financial Accountability Act.

Office of the Chief Financial Officer:

Andrew Maner, Chief Financial Officer
Eugene Schied, Deputy Chief Financial Officer
AnneMarie Bruen, OCFO Chief of Staff
John McNamara, Director Office of Financial Management, OCFO
Mike Wetklow, Financial Accountability Act Program Manager, OCFO
Dale Amidon, Office of Financial Management, OCFO
Rich Aaronson, Office of Financial Management, OCFO
James Eun, Office of Financial Management, OCFO
Marilyn Evans, Office of Financial Management, OCFO
Bill Mason, Office of Financial Management, OCFO
Otis France, Office of Budget, OCFO
John Makepeace, Office of Resource Management Transformation Office, OCFO
Veronica Epley, Office of Program Analysis and Evaluation, OCFO
Carl Erickson, Office of Program Analysis and Evaluation, OCFO
Steve Pecinovsky, Office of Audit Liaison, OCFO

Component Financial Management Community:

James Alfredo, Information Analysis and Infrastructure Protection
Sean Richey, Border and Transportation Security
Mari Boyd, U.S. Customs and Border Protection
Mitch Demich, U.S. Immigration and Customs Enforcement
James Landolt, U.S. Immigration and Customs Enforcement
David Lanagan, Transportation Security Administration
Julie Martin, Federal Law Enforcement Training Center
Ellen Wesley, Office of State and Local Government Coordination and Preparedness
Kaye McTighe, Emergency Preparedness and Response – FEMA
Margaret Chan, Emergency Preparedness and Response – FEMA
Marco Terango, Science & Technology
Holly Mathis, U.S. Coast Guard
Dale Burkett, U.S. Secret Service
Kathleen Stanley, U.S Citizenship and Immigration Services
Richard Reilly, Office of the Inspector General
Sue Schwendiman, Office of the Inspector General

Cross Functional Community:

Ann Albin, Office of the Chief Human Capital Officer
Wayne Bavery, Office of the Chief Information Officer
Pamela Boteler, Office of the Chief Human Capital Officer
Janet Dobbs, Office of the Chief Administrative Services Officer
Vicki Granat, Office of the Chief Procurement Officer
Van Pace, Office of the Chief Procurement Officer
Michael Russell, Office of General Counsel
Ann Van Houten, Office of the Chief Procurement Officer

Homeland Security

Additional Information and Copies

To obtain additional copies of this guide, call the Department's Office of Financial Management at (202) 205-2857, or visit the Department of Homeland Security Public Website at http://www.dhs.gov